Honeywell

MX7 Tecton™ Mobile Computer

with Microsoft® Windows® Mobile 6.5

User's Guide

Disclaimer

Honeywell International Inc. (“HII”) reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult HII to determine whether any such changes have been made. The information in this publication does not represent a commitment on the part of HII.

HII shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing, performance, or use of this material.

HII disclaims all responsibility for the selection and use of software and/or hardware to achieve intended results.

Web Address: www.honeywellaidc.com

Trademarks

RFTerm is a trademark or registered trademark of EMS Technologies, Inc. in the United States and/or other countries.

Microsoft® Windows®, ActiveSync®, MSN, Outlook®, Windows Mobile®, the Windows logo, and Windows Media are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Marvell® is a registered trademark of Marvell Technology Group Ltd., or its subsidiaries in the United States and other countries.

Summit Data Communications, the Laird Technologies Logo, the Summit logo, and “Connected. No Matter What” are trademarks of Laird Technologies, Inc.

The Bluetooth® word mark and logos are owned by the Bluetooth SIG, Inc.

microSD and microSDHC are trademarks or registered trademarks of SD-3C, LLC in the United States and/or other countries.”

Symbol® is a registered trademark of Symbol Technologies. MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license.

Hand Held is a trademark of Hand Held Products, Inc., a subsidiary of Honeywell International.

RAM® and RAM Mount™ are both trademarks of National Products Inc., 1205 S. Orr Street, Seattle, WA 98108.

Wavelink®, the Wavelink logo and tagline, Wavelink Studio™, Avalanche Management Console™, Mobile Manager™, Mobile Manager Enterprise™ are trademarks of Wavelink Corporation, Kirkland.

Wi-Fi®, WMM®, Wi-Fi Mutlimedia™, Wi-Fi Protected Access®, WPA™, WPA2™ and the Wi-Fi CERTIFIED™ logo are trademarks or registered trademarks of Wi-Fi Alliance.

Acrobat® Reader © 2014 with express permission from Adobe Systems Incorporated.

Other product names or marks mentioned in this document may be trademarks or registered trademarks of other companies and are the property of their respective owners.

Patents

For patent information, please refer to www.hsmpats.com.

Table of Contents

Chapter 1 - MX7 Tecton Agency Compliance

Chapter 2 - Getting Started

Chapter 3 - Hardware Configuration

Chapter 4 - Power Modes and Batteries

Chapter 5 - Software Configuration

Chapter 6 - AppLock (Application Locking)

Chapter 7 - Bluetooth Configuration

Chapter 8 - Data Collection Wedge

Chapter 9 - Enhanced Launch Utility

Chapter 10 - Enabler Installation and Configuration

Chapter 11 - Wireless Network Configuration

Chapter 12 - Keymaps

Chapter 13 - Battery Charger

Chapter 14 - Cradles

Chapter 15 - Technical Specifications

Chapter 16 - Customer Support

1

MX7 Tecton Agency Compliance

MX7 Tecton mobile computers meet or exceed the requirements of all applicable standards organizations for safe operation. However, as with any electrical equipment, the best way to ensure safe operation is to operate them according to the agency guidelines that follow. Read these guidelines carefully before using your MX7 Tecton.

This documentation is relevant for the following models: Tecton, TectonCS.

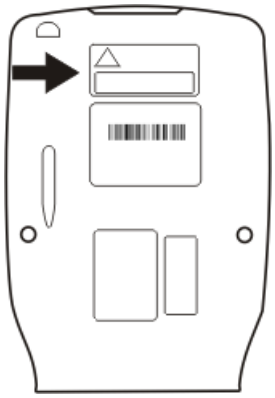
Caution: ⚠	RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. The battery should be disposed of by a qualified recycler or hazardous materials handler. Do not incinerate the battery or dispose of the battery with general waste materials.

Laser Warnings

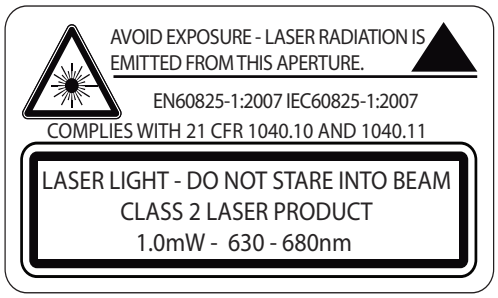
- Do not look into the laser's lens.
- Do not stare directly into the laser beam.
- Do not remove the laser caution labels from the Tecton.
- Do not connect the laser bar code aperture to any other device. The laser bar code aperture is certified for use with the MX7 Tecton only.

Caution: ⚠	Laser radiation when open. Read the caution labels. Use of controls, adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.

Laser Label Location



If the following label is attached to your product, it indicates the product contains an engine with a laser aimer:



Laser Safety Statement

This device has been tested in accordance with and complies with IEC60825-1 ed2 (2007). Complies with 21 CFR 1040.10 and 1040.11, except for deviations pursuant to Laser Notice No. 50, dated June 24, 2007.

LASER LIGHT, DO NOT STARE INTO BEAM, CLASS 2 LASER PRODUCT, 1.0 mW MAX OUTPUT: 630-680nM.

Model Number and Serial Number Labels

The model (item) number and serial number for the terminal are located on labels affixed to the back of the terminal.

FCC Part 15 Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio or television technician for help.

If necessary, the user should consult the dealer or an experienced radio/television technician for additional suggestions. The user may find the following booklet helpful: “Something About Interference.” This is available at FCC local regional offices. Honeywell is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Honeywell. The correction is the responsibility of the user.

Caution: Any changes or modifications made to this equipment not expressly approved by Honeywell may void the FCC authorization to operate this equipment.

FCC 5GHz Statement

LAN devices are restricted to indoor use only in the band 5150-5250 MHz. For the band 5600-5650 MHz, no operation is permitted.

When using IEEE 802.11a wireless LAN, this product is restricted to indoor use, due to its operation in the 5.15- to 5.25-GHz Frequency range. The FCC requires this product to be used indoors for the frequency range of 5.15 GHz to 5.25 GHz to reduce the potential for harmful interference to co-channel mobile satellite systems. High-power radar is allocated as the primary user of the 5.25- to 5.35-GHz and 5.65- to 5.85-GHz bands. These radar stations can cause interference with and/or damage to this device.

Canadian Compliance

This ISM device complies with Canadian RSS-210.

Operation is subject to the following conditions:

1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation.

This Class B digital apparatus complies with Canadian ICES-003.

CE Mark

The CE marking indicates compliance with the following directives:

- 1995/5/EC R&TTE
- 2011/65/EU RoHS (Recast)

In addition, complies to 2006/95/EC Low Voltage Directive, when shipped with recommended power supply. European contact::

CE Hand Held Products Europe BV
Nijverheidsweg 9-13
5627 BT Eindhoven
The Netherlands

Honeywell shall not be liable for use of our product with equipment (i.e., power supplies, personal computers, etc.) that is not CE marked and does not comply with the Low Voltage Directive.

RF Notices

This device (FCC ID: KDZLXE-MX7T and IC ID: 1995B-LXEMX7T) contains transmitter Module FCC ID: TWG-SD-CMSD30AG and IC ID: 6616A-SDCMSD30AG.
This device does not transmit simultaneously on adjacent or non-adjacent channels.

RF Safety Notice

Caution:

This device was tested for typical body-worn operation. Use only Honeywell tested and approved accessories to ensure FCC Compliance. The use of third-party accessories may not comply with FCC RF exposure compliance requirements, and should be avoided. To comply with FCC RF exposure requirements, this device must be operated in the hand with a minimum separation distance of 2.5 cm (0.9842 inch) or more from a person's body.

Bluetooth

Bluetooth® Class II

Honeywell Scanning & Mobility Product Environmental Information

Refer to www.honeywellaidc.com/environmental for the RoHS / REACH / WEEE information.

Dealer License - Republic of Singapore

Complies with
IDA Standards
DA103458

Vehicle Power Supply Connection Safety Statement

Vehicle Power Supply Connection: If the supply connection is made directly to the battery, a 10A slow-blow fuse should be installed in the positive lead within 5 inches (12.7 cm) of the battery positive (+) terminal.

2 Getting Started

Overview

The MX7 Tecton™ is a rugged, portable, hand-held mobile computer capable of wireless data communications. The MX7 Tecton can transmit information using an 802.11 network card and it can store information for later transmission through an RS232 or USB port. The MX7CS (Cold Storage) device functions normally in various temperature ranges.

The MX7 Tecton is vertically oriented and features backlighting for the display. Keypads are available in 55-key alphanumeric and 32-key numeric-alpha versions.

This device can be scaled from a limited function batch computer to an integrated wireless scanning computer. A trigger handle is available as an accessory.

The stylus attached to the hand strap is used to assist in entering data and configuring the device. Protective film for the touch screen is available as an accessory.

The MX7 Tecton is powered by a 2200 mAh Lithium-Ion main battery pack and an internal Super-capacitor (Super-cap) battery.

Note: Contact Technical Assistance (page 16-1) for upgrade availability if your application or control panels are not the same as the application or control panels presented in this guide.

About this Guide

This MX7 Tecton User's Guide provides instruction for the system administrator to follow when configuring a MX7 Tecton. Also included are setup and use instructions for the MX7 Tecton Battery Charger, Desktop Cradle, Passive Vehicle Mounted Cradle, and Powered Vehicle Mounted Cradle.

Note: The MX7 Tecton may have a Microsoft Windows CE 6 or Microsoft Windows Mobile 6.5 operating system. This guide is for the MX7 Tecton with a Windows Mobile 6.5 operating system

Out of the Box

After you open the shipping carton verify it contains the following items:

- MX7 Tecton
- Rechargeable battery
- Hand Strap (attached to the MX7 Tecton)
- Quick Start Guide
- Getting Started Disc

If you ordered accessories for the MX7 Tecton, verify they are also included with the order. Keep the original packaging material in the event the MX7 Tecton should need to be returned for service. For details, see Product Service and Repair (page 16-1)

Initial Setup for MX7 Tecton

Following are steps you might take when setting up a new MX7 Tecton. Follow the links for further instruction for each step. Contact *Technical Assistance* (page 16-1) if you need additional help.

Note: Installing or removing accessories should be performed on a clean, well-lit surface. When necessary, protect the work surface, the MX7 Tecton, and components from electrostatic discharge.

Hardware Setup

1. Connect accessories e.g., hand strap (if necessary), trigger handle, etc.
2. Provide a power source:
   - Insert a fully charged main battery.
   - Connect a power cable (USB/Power or Serial/Power).
   - Place the MX7 Tecton in a powered desktop or vehicle mounted cradle.
3. Press the Power key.

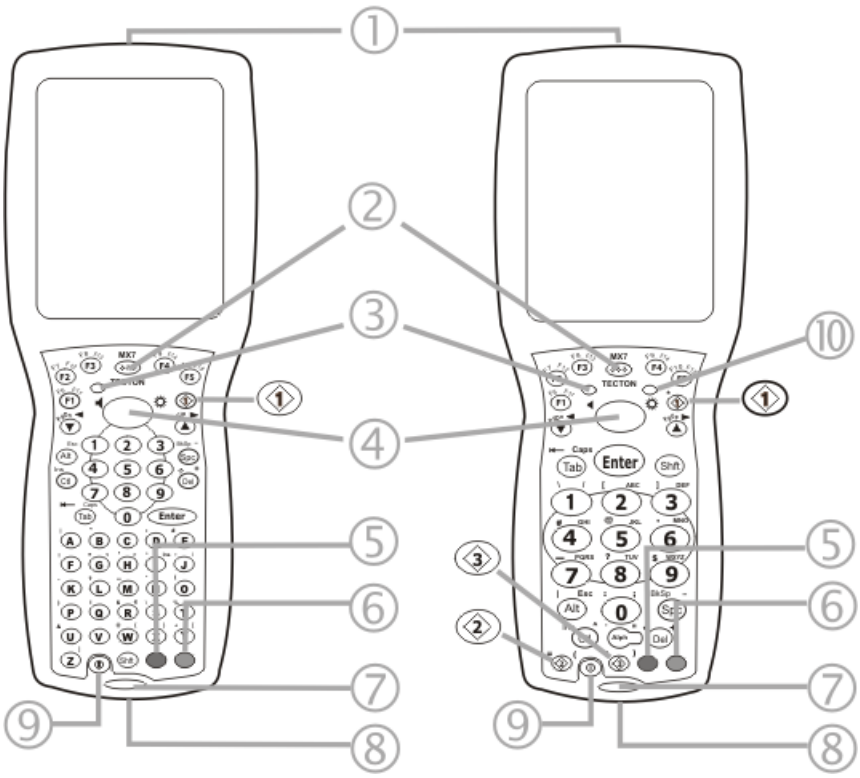
Software Setup

Hardware setup should be completed before starting software setup.

1. Calibrate Touch display.
2. Set Date and Time Zone.
3. Set Power Timers.
4. Set Speaker Volume.
5. Pair Bluetooth devices.
6. Set Wireless client parameters.
7. Set terminal emulation parameters.
8. Set AppLock parameters.
9. Set DCWedge parameters.

Components

Front View

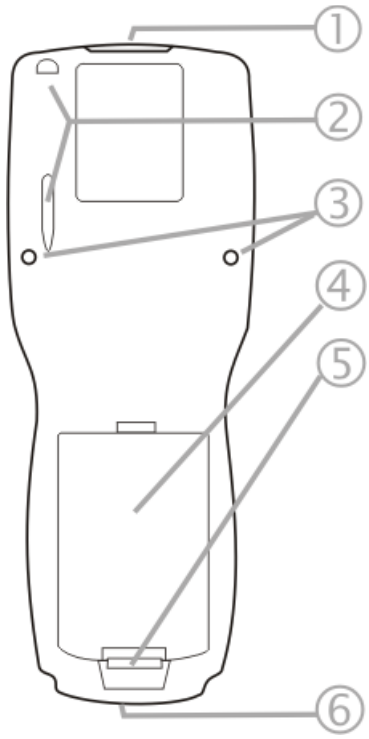


55-key Keypad 32-key Keypad

1. Scanner/Imager Aperture
2. Speaker
3. System Status LED
4. Scan Button
5. Orange Key (Sticky Key)
6. Blue Key (Sticky Key)
7. Scan Status LED
8. Cable Port
9. On / Off Button
10. Alpha Lock LED (32 Key keypad only)

Diamond Keys

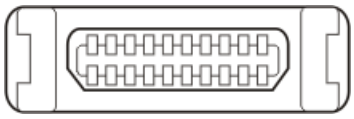
Back View



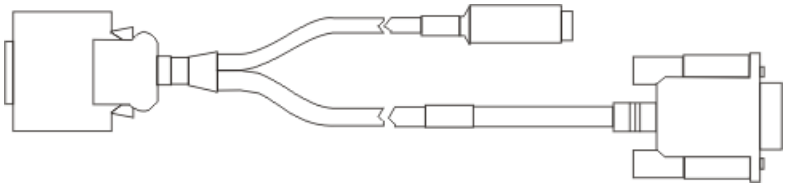
1. Scanner/Imager Aperture
2. Stylus and Stylus Pocket
3. Trigger Handle Attach Points
4. Main Battery
5. Battery Fastener
6. Cable Port

I/O Port and Cables

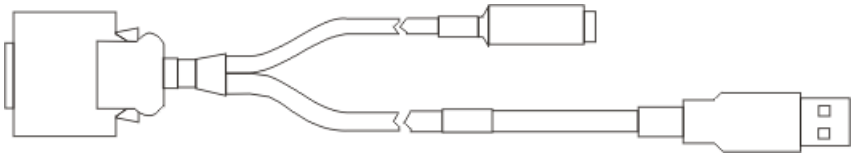
Input / Output Port (I/O)



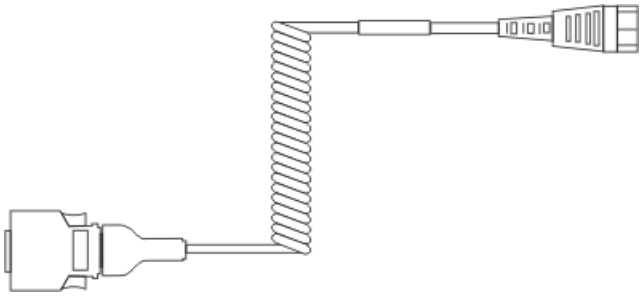
Cable: Multipurpose RS232 and Power (MX7055CABLE)



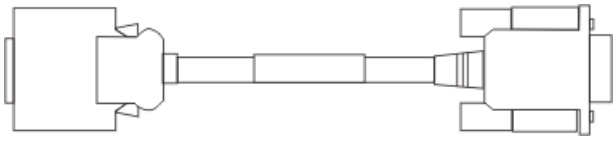
Cable: Multipurpose USB and Power (MX7052CABLE)



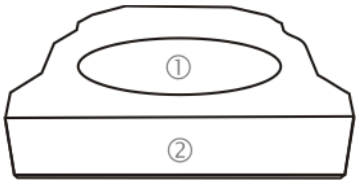
Adapter/Cable: Audio (MX7060CABLE)



Adapter: RS232 PC port to D9 male (MX7058CABLE)



Scanner / Imager Aperture

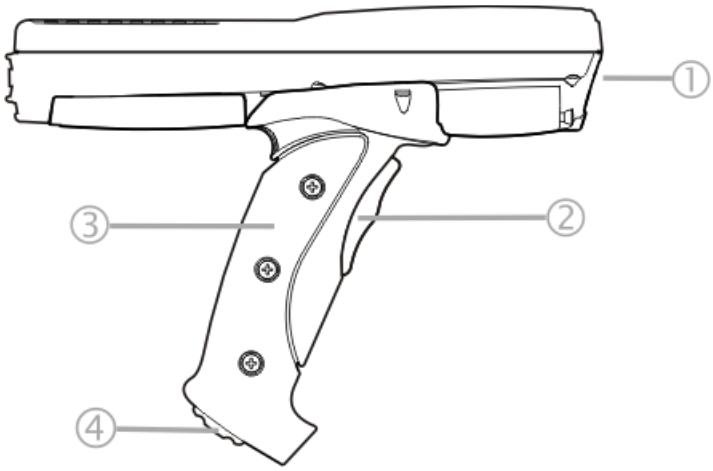


1. Scanner Aperture
2. MX7 Tecton Front

Caution: Never stare directly into the beam aperture.

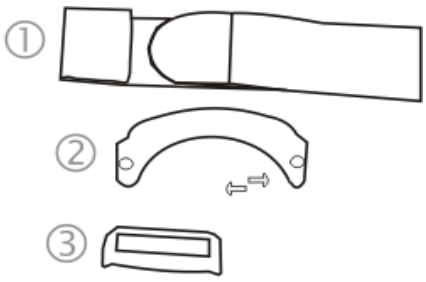
If ***Continuous Scan Mode*** has been enabled (disabled by default, setting can be changed by user), the laser is always on and decoding and the laser beam is emitted continuously.

Handle



1. Imager / Scanner Aperture
2. Trigger
3. Handle
4. Tether Attach Point

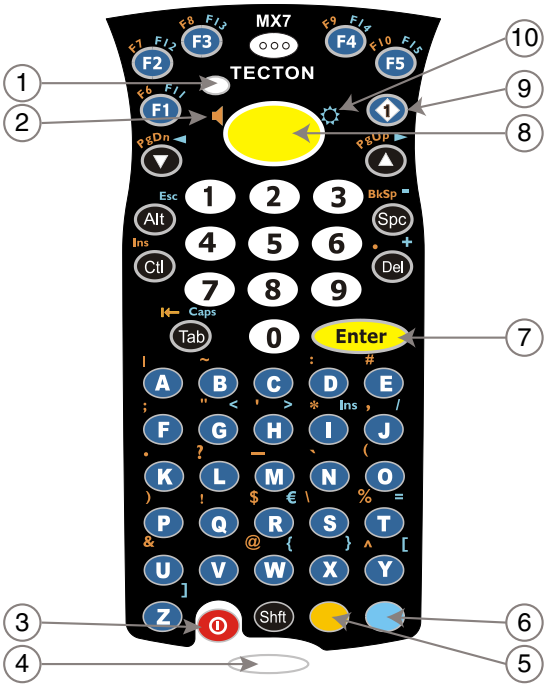
Handstrap



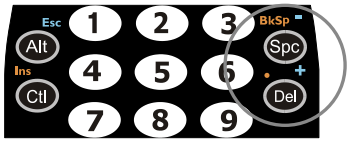
1. Handstrap
2. Handstrap Retainer Bracket and mounting screws
3. Handstrap Clip

Keypads

55 Key Primary Delete ANSI Keypad

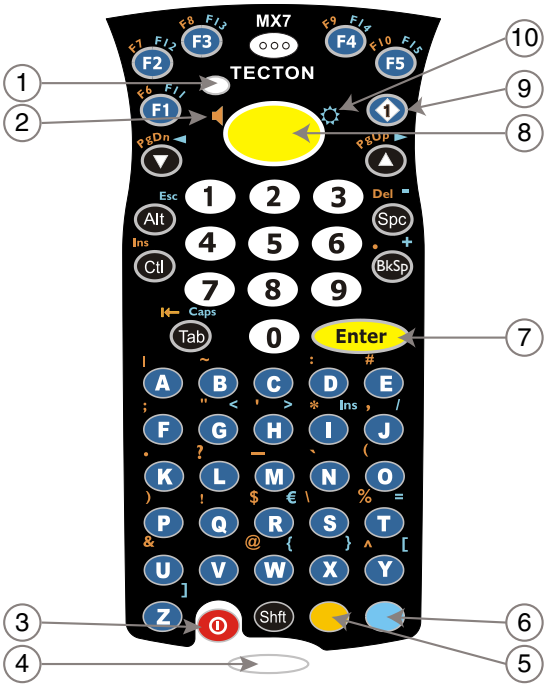


1. System Status LED
2. Volume Control Icon
3. On Off Button
4. Scan Status LED
5. Orange Key (Sticky Key)
6. Blue Key (Sticky Key)
7. Enter Key
8. Scan Button
9. Diamond Key
10. Display Brightness Icon

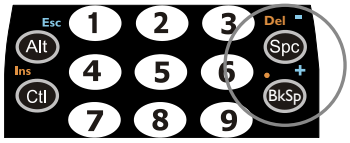


Spc and Del key location

55 Key Primary Backspace ANSI Keypad

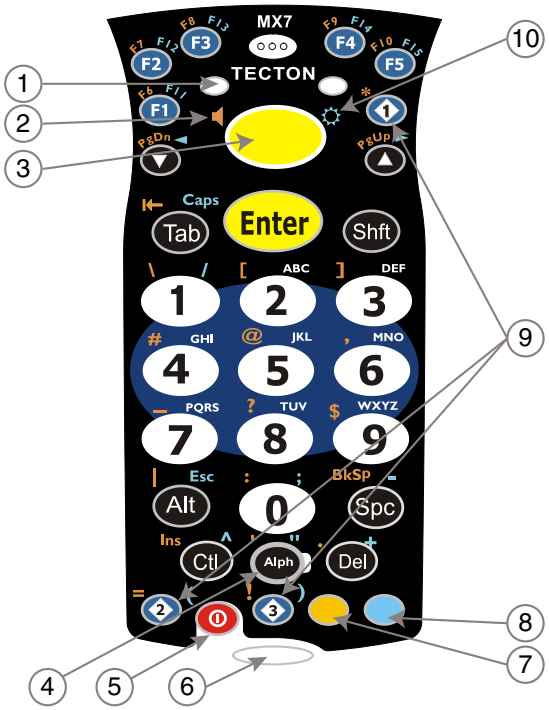


1. System Status LED
2. Volume Control Icon
3. On Off Button
4. Scan Status LED
5. Orange Key (Sticky Key)
6. Blue Key (Sticky Key)
7. Enter Key
8. Scan Button
9. Diamond Key
10. Display Brightness Icon



Spc and Bksp key location

32 Key Numeric-Alpha Keypad



1. System Status LED
2. Alpha Status LED
3. Diamond Keys
4. Scan Button
5. Enter Key
6. Alph Key
7. Orange Key (Sticky Key)
8. Blue Key (Sticky Key)
9. On Off Button
10. Scan Status LED

Locking and Unlocking the MX7 Tecton

Locking the MX7 Tecton

The MX7 Tecton can be locked manually by tapping **Start > Lock**. By default, this option is included on the Start screen at the bottom of the screen. Care should be taken to not accidentally tap this area of the Start screen.

Note: Review the Unlock process before locking the MX7 Tecton.

Lock can be removed from the Today screen by selecting **Start > Settings > Today >** Items (page 5-22) tab. Deselect *Device Lock*.

The MX7 Tecton can also be configured to Lock automatically after a defined period of inactivity. This setting is accessed via **Start > Settings > Lock > Password** tab. By default, this option is Disabled.

The password and hint are configured by selecting **Start > Settings > Lock** > Password (page 5-16) and Hint (page 5-17) tabs.

Unlocking the MX7 Tecton

When the MX7 Tecton is locked, the Start screen displays *Unlock* at the lower part of the screen.

- If there *is no password* or PIN set, tap Unlock on the next screen to unlock the MX7 Tecton. The MX7 Tecton is returned to normal operation.
- If there *is a password* or PIN set, enter the password/PIN and tap Unlock. If several unsuccessful attempts are made, the MX7 Tecton may be configured to display a password hint.

Rebooting the MX7 Tecton

When the Desktop/Start screen is displayed or an application begins, the power up sequence is complete. If you have previously saved your settings, they will be restored on reboot. Application panel changes are saved when **OK** is tapped on an application properties panel.

During the processes that follow there may be small delays while MX7 Tecton wireless clients connect to the network and Bluetooth relationships establish or re-establish.

Suspend / Resume

Quickly tapping the Power key places the MX7 Tecton in Suspend mode. Quickly tapping the Power key again, pressing any key, pressing the trigger (on the trigger handle), or tapping the touch screen, returns the MX7 Tecton from Suspend and to the exact state before the Power key press. The System LED blinks green when the video display is Off (and the device is not in Suspend Mode or critical suspend).

Warmboot

A warmboot reboots the MX7 Tecton without erasing any registry data. Configuration settings and data in RAM are preserved during a warmboot. Network sessions are lost and any data in running applications that has not been previously saved may be lost. CAB files already installed remain installed.

- Using the Registry control panel, tap the Warmboot button. The MX7 Tecton immediately warmboots.

Restart

The OS and CAB files are reloaded. Restart erases the contents of RAM but preserves all registry configuration settings. Any files that are stored only in RAM drives will be lost. Restart erases any user-stored applications or data, but preserves anything stored on the System drive in flash (which are files explicitly copied to the System folder, plus the registry files created by the OS). All CABs and applications that are configured are reinstalled by the Launch utility. Touch screen calibration data is preserved. Network sessions are lost, and any data in running applications that has not been specifically sent to storage may be lost.

- Tap the Restart button on the Registry control panel. The operating system performs the operation and the MX7 Tecton restarts.
- An alternate method to Restart is to hold down the Blue key, the Scan key and the Power key until the screen blanks. Release the keys and the MX7 restarts (may also be called a cold boot). Be sure the press the Scan key, not the Enter key. Pressing the Enter key begins a warmboot function instead of a coldboot function.

Clean Boot / Reset

Important -- Because of the extreme nature of resetting the Windows Mobile device to factory default settings, this process should be used only as an emergency procedure and suspend/resume or restart should be used whenever necessary.

To reset ***all*** Windows Mobile device configuration to factory defaults:

1. Hold down the Blue + Scan + Power keys at the same time. After the key sequence is complete, the display turns solid white. Be sure to press the Scan key, not the Enter key.
2. Release the keys and immediately press and hold the Enter + Scan keys. After the keypress, the display turns dark. (If these keys are not pressed immediately the MX7 Tecton performs a Cold Boot. Wait until the MX7 Tecton boots and try again.)
3. Release the Reset key sequence. A message is displayed stating the change is in process. If the message does not appear, try again.

When all programs have finished loading, the Windows Mobile Start screen is displayed. If prompted, tap the touch screen to set up your Windows Mobile based device.

Inserting and Removing the Battery Pack

Note: The battery should not be replaced in a dirty, harsh or hazardous environment. When the battery is not connected to the MX7 Tecton, any dust or moisture that enters the battery well or connector may transfer to the battery/well terminals, potentially causing damage. Only use Honeywell batteries as replacements: MX7A380BATT / MX7392BATT or a Low Temperature (CS) Battery : MX7A381BATT / MX7393BATT / MX7396BATTERY.

The MX7 Tecton will not function unless the battery pack is in place and securely latched. Any work in progress should be saved prior to replacing the battery pack.

Be sure to place the unit in Suspend Mode before removing the battery. Failing to properly place the device in Suspend mode will result in a loss of all unsaved data.

An MX7 Tecton will retain data, while the main battery is removed and replaced with a fully charged main battery, for 5 minutes.

Note: When internal battery power is Low or Very Low connect the AC/DC adapter to the MX7 Tecton before replacing the main battery.

Inserting the Battery

To insert the main battery, complete the following steps:

1. Place the MX7 Tecton in Suspend Mode (if On).
2. Detach the bottom hook of the handstrap (if installed).
3. Tilt the end (without the latch) of the fully charged battery pack into the upper end of the battery compartment, and firmly press the other end down until it is fully inserted into the battery compartment
4. Push down on the battery until the retaining clip clicks into place. The MX7 Tecton draws power from the battery immediately upon successful connection.
5. Replace the handstrap clip in its holder (if installed).

Removing the Battery

To remove the battery, complete the following steps:

1. Place the MX7 Tecton in Suspend mode (if On).
2. Detach the bottom hook of the handstrap (if installed).
3. Slide the battery retaining clip down to release the main battery.
4. Pull the battery up and out of the battery compartment.
5. Place the discharged battery pack in a powered battery charger to re-charge.

Charging the Main Battery

Note: The MX7 Tecton Battery Charger is designed for an indoor, protected environment.

New batteries must be fully charged prior to use.

The main battery can be recharged in an AC powered Battery Charger after the battery has been removed from the MX7 Tecton or its packing material when new.

The main battery can be recharged while it is in the MX7 Tecton:

- by connecting the MX7 Tecton AC power adapter to the I/O connector at the base of the MX7 Tecton.
- by docking the MX7 Tecton in a powered desk cradle.
- by docking the MX7 Tecton in a powered vehicle cradle.
- or by connecting the car power adapter (CLA) to the I/O connector at the base of the MX7 Tecton.

Note: An uninterrupted external power source (wall AC adapters) transfers power to the computer's internal charging circuitry which, in turn, recharges the main battery and internal battery. Frequent connection to an external power source, if feasible, is recommended to maintain internal battery charge status as the internal battery cannot be recharged by a dead or missing main battery.

LEDs and Indicators

The **Scan Status** oval shaped indicator is situated below the keypad and next to the On button.

LEDs (Light Emitting Diodes) are located on the front of the MX7 Tecton. They are:

- System Status LED indicates power management status. It is located at the top left of the keypad, below the F3 key.
- Alpha Mode Status LED applies to the 32-key keypad only. It is located below the F4 key on the 32-key keypad.

System Status LED

Blinking Red	Battery power fail; critical suspend mode.
Steady Red	Main battery low.
Blinking Green	Display turned off.
Yellow / Amber	A few seconds when Power key is pressed.
No Color	No user intervention required.

Alpha mode Status LED

Steady Green	Device is in “Alpha” character input mode.
No Color	Device is in “Numeric” key input mode.

Scan Status Indicator

Steady Green	Good scan.
Steady Amber	Decoder engine storing changed parameters.
Steady Red	Scan in progress.
No Color	Scanner / Imager ready for use or no scanner installed.

Toggle Vibrate Indicator

The vibration motor is activated when a scan is completed successfully (good scan vibration) or with a failure (scan key released before good scan, timeout, or rejected because of Data Options configuration). The vibrations can be detected under the handstrap or through the trigger handle.

Vibrate indicator is toggled on and off in the Data Collection application, using the Notification tab. Toggle the vibrate indicator on or off by tapping the desired radio button for Good Scan Vibration and Bad Scan Vibration.

Options are: Off, Short, Medium or Long.

Vibration can also be adjusted by tapping the speaker icon in the top right corner of the Start screen. A Volume window opens. Tap the Vibrate radio button to toggle vibration on and off. Vibration duration can be set using the Data Collection control panels.

Tapping the Touch Screen with a Stylus

Note: Always use the point of the stylus for tapping or making strokes on the touch screen.

Never use an actual pen, pencil, or sharp/abrasive object to write on the touch screen.

Hold the stylus as if it were a pen or pencil. Touch an element on the screen with the tip of the stylus then lift the stylus from the screen. Using a stylus is similar to moving the mouse pointer then left-clicking icons on a desktop computer screen.

Firmly press the stylus into the stylus holder when the stylus is not in use. There is a stylus holder in the hand strap and the trigger handle. A stylus replacement kit is available.

Using the stylus to tap icons on the touch screen is the basic action that can:

- Open applications.
- Choose menu commands.
- Select options in dialog boxes or drop-down boxes.
- Drag the slider in a scroll bar.
- Select text by dragging the stylus across the text.
- Place the cursor in a text box prior to typing in data.
- Place the cursor in a text box prior to retrieving data using a bar code decoder or an input/output device connected to a serial port on a cradle.

Calibrating the Touch Screen

If the touch screen is not responding properly to stylus taps, you may need to recalibrate the touch screen.

Recalibration involves tapping the center of a target. If you miss the center, keep the stylus on the screen, slide it over the target's center, and then lift the stylus.

To recalibrate the screen, select **Start > Settings > System** > Screen (page 5-46) > **General** tab. To begin, tap the Align Screen button on the display with the stylus.

Follow the instructions on the screen and press the Enter key to save the new calibration settings or press Esc to cancel or quit.

Setting the Display Backlight Timer

The backlight settings use Honeywell-determined default timeouts. Different timeouts can be set for the backlights when using main battery or external power. The backlights timer can be disabled for a particular mode by unchecking a check box. When the backlight timer is disabled (check box is unchecked), the backlight never turns off (or dims) in that mode.

Default values are 30 seconds for Battery, 1 minute for External. Brightness level default value is 60% for the keypad and display.

When the backlight timer expires, the display backlight and the display are Off, as is the keypad backlight. The backlights are turned on when the touch screen is tapped or a button is pressed. Adjust these settings using the Backlight control panel.

Applying the Touch Screen Protective Film

1. Clean the touch screen of fingerprints, lint particles, dust and smudges.
2. Remove the protective film from its container. Remove any protective backing from the film sheet by lifting the backing from a corner of the film. Discard the backing.
3. Apply the film to the touch screen starting at one side and smoothing it across the display.
4. If air bubbles appear, raise the film slightly and continue smoothing the film across the display until it covers the glass surface of the display.
5. If dust, lint or smudges are trapped between the protective film and the glass display, remove the protective film, clean the display and apply the protective film again.

Setting the Date and Time Zone

Note: The first time the MX7 Tecton is powered up, or the device powers up from a reset/cold boot, the time may be reset to the factory default value.

Set the current date, time, time zone and assign a daylight savings location using control panels. Or double-tap the Date icon in the taskbar to begin.

There is very little functional change from standard desktop PC Date/Time Properties options. Adjust the settings and tap the **OK** button or the Apply button to save changes to the registry. Any changes take effect immediately.

Setting Speaker Volume

The speaker is located on the front of the device, between MX7 and Tecton.

Speaker volume can be adjusted to a comfortable level for the listener by using key presses or by changing settings in a control panel. Speaker sounds can be disabled.

Using the Keypad

Note: Speaker sounds must be enabled before the following key sequences can adjust the volume.

The volume is increased or decreased one step each time the volume key sequence is pressed.

To adjust speaker volume:

- Tap the Orange key then the Scan key to enter volume change mode.
- Use the Up Arrow and Down Arrow keys. A beep is emitted at each arrow key press. When the volume reaches maximum level, two extra beeps are emitted.
- Press any key, except the keys you used to adjust the volume, to exit.

Volume control using a keypad key press has six volume settings that match those supported by the control panel. Volume does not “roll-over” from minimum to maximum or from maximum to minimum. Continuously holding down the up or down arrow keys does not cause an automatic repeat of the up (or down) arrow key.

Using a Control Panel

Sounds for Events and Programs are enabled by default. Notifications are disabled by default. See Sounds & Notifications (page 5-20)

1. Tap the speaker icon in the top right corner of the Start screen. A Volume window opens.
2. Move the slider up and down to adjust the speaker volume.
3. If desired, tap the Off radio button to turn sounds off.
4. If desired, tap the Vibrate radio button to turn Vibrate on. Vibrate is off by default.

Setting Terminal Emulation Parameters

Before you make a host connection, you will, at a minimum, need to know:

- the alias name or IP address (Host Address) and
- the port number (Telnet Port) of the host system to properly set up your host session.

1. Make sure the MX7 Tecton network settings are configured and functional. If you are connecting over wireless LAN (802.11*x*), make sure your MX7 Tecton is communicating with the Access Point.
2. From **Start > Programs,** run RFTerm or tap the RFTerm icon on the desktop.
3. Select **Session > Configure** from the application menu and select the host type that you require. This will depend on the type of host system that you are going to connect to; i.e., 3270 mainframe, AS/400 5250 server or VT host.
4. Enter the Host Address of the host system that you wish to connect to. This may either be a DNS name or an IP address of the host system.
5. Update the telnet port number, if your host application is configured to listen on a specific port. If not, use the default telnet port.
6. Select **OK**.
7. Select **Session > Connect** from the application menu or tap the Connect button on the Tool Bar.
8. Upon a successful connection, you should see the host application screen displayed.

To change options such as Display, Colors, Cursor, Bar Code, etc., refer to these sections in the *RFTerm User's Guide* for complete descriptions of these and other features.

Using the AppLock Switchpad

Note: The touch screen must be enabled.

Switchpad Menu

Switchpad Icon

Tap the switchpad icon in the taskbar.

A checkmark on the switchpad menu indicates applications currently active or available for Launching by the MX7 Tecton user. When Keyboard, on the Switchpad Menu, is selected, the default input method (Input Panel, Transcriber, or custom input method) is activated.

Using the Keypad

One switch key sequence (or hotkey) is defined by the Administrator for the end-user to use when switching between locked applications. This is known as the **Activation key**.

When the Activation key sequence is pressed on the keypad, the next application in the AppLock configuration is moved to the foreground and the previous application moves to the background. The previous application continues to run in the background. MX7 Tecton key presses affect the application in focus only.

Using the Touch Screen

The Switchpad Menu figure shown above is an example and is shown only to aid in describing how the user can switch between applications using a stylus.

When the user taps the Switchpad icon with the stylus, a menu pops up listing the applications available to the user. The user can tap an application name in the popup menu and the selected application is brought to the foreground. The previous application continues to run in the background. Stylus taps affect the application in focus only. When you need to use the Input Panel, tap the Keyboard option. Input Panel taps affect the application in focus only.

Using the Input Panel / Virtual Keyboard

The input panel / virtual keyboard is always available when needed e.g., text entry.

Place the cursor in the text entry field and, using the stylus:

- Tap the Shift key to type one capital letter.
- Tap the CAPS key to type all capital letters.
- Tap the áü key to access symbols.

Some applications do not automatically display the Input Panel. In this case, do the following to use the Input Panel:

	Keyboard icon in the taskbar
	Transcriber icon in the taskbar
	Block recognizer or Letter recognizer icon in the taskbar

1. If the keyboard icon is not displayed in the taskbar, tap the icon which is present.
2. Tap the up arrow beside the icon and select **Keyboard**.
3. Tap the Keyboard icon in the taskbar. Tapping the Keyboard icon in the taskbar is a toggle action (On/Off).
4. Move the cursor into the text entry field when you want to enter data using the Input Panel.
5. When finished entering data, tap the icon in the Taskbar again.

Connecting to Bluetooth Devices

Before connecting to Bluetooth Devices:

- The system administrator, using the options on the EZPair (or LXEZ Pairing) control panel has discovered, paired, connected and disconnected Bluetooth devices for the MX7 Tecton.
- The system administrator has enabled and disabled EZPair (or LXEZ Pairing) parameters for the MX7 Tecton.
- The system administrator has also assigned a Computer Friendly Name using the EZPair (or LXEZ Pairing) control panel for the MX7 Tecton.

To connect Bluetooth devices, the MX7 Tecton should be as close as possible and in direct line of sight (distances up to 32.8 feet or 10 meters) with the targeted Bluetooth device during the discovery and pairing process.

If the Bluetooth devices are in Suspend, tap the power key to wake the MX7 Tecton.

Using the correct procedure, wake the targeted Bluetooth device if necessary.

There may be audible or visual signals as both devices discover and pair with each other.

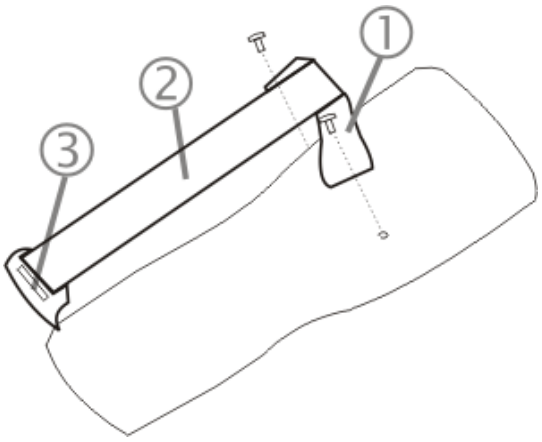
Taskbar Bluetooth Indicator

	MX7 Tecton is connected to one or more of the targeted Bluetooth device(s).
	MX7 Tecton is not connected to any Bluetooth device. MX7 Tecton is ready to connect with any Bluetooth device. MX7 Tecton is out of range of all paired Bluetooth device(s). Connection is inactive.

There may be audible or visual signals from paired devices as they move back into range and re-connect with the Bluetooth client in the MX7 Tecton.

Attaching the Handstrap

Note: Either the trigger handle is attached to the MX7 Tecton or the handstrap is attached, not both. In the absence of a trigger handle, the handstrap should be used at all times. The handstrap is pre-installed on a MX7 Tecton.



1. Handstrap Retainer Bracket
2. Handstrap and tethered stylus
3. Handstrap Clip

Tool Required: Phillips #1 screwdriver (not supplied)

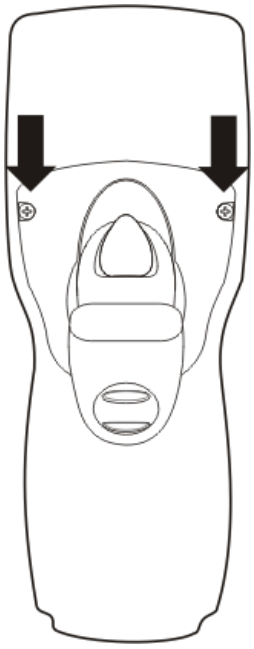
1. Place the MX7 Tecton with the screen facing down, on a flat stable surface.
2. Attach the handstrap retainer bracket to the MX7 Tecton with the screws and washers provided.
3. Slip the Handstrap Clip into the bracket at the base of the MX7 Tecton.
4. Making sure the closed loop fastener surfaces on the handstrap are facing up, slide the strap through the pin in the bottom bracket and the clip.
5. Fold each end of the strap over so that the closed loop fastener surfaces mate evenly.
6. Test the strap's connection making sure the MX7 Tecton is securely connected to each end of the handstrap's connectors.

Check the closed loop fastener, retainer bracket and clip connections frequently. If they have loosened, they must be tightened or replaced before the MX7 Tecton is placed into service again.

Attaching the Trigger Handle

Either the trigger handle or the handstrap is attached, not both. Honeywell recommends that, in the absence of a trigger handle, the handstrap be used at all times.

Pressing the trigger on the trigger handle activates the integrated scanner and functions the same as the Scan button on the keypad. With the trigger handle installed the Scan key on the keypad remains active. A trigger press duplicates the Scan button press operation.



- The handle is built of a durable, flexible plastic.
- The handle will not detach from the MX7 Tecton if the unit is dropped.
- The trigger handle is a mechanical device. Battery or external A/C power is not required for operation.
- The trigger handle does not need to be removed when replacing the main battery pack.
- The trigger handle might also be called a pistol grip.

Tool required: Torque wrench capable of torquing to 3±1 in/lb (.34±.11 N/m).

1. Place the MX7 in Suspend.
2. Place the MX7 Tecton with the screen facing down, on a flat stable surface.
3. Remove the handstrap, if installed. Tool required: Phillips #1 screwdriver.
4. Remove the main battery.
5. Slide the locking tab on the underside of the trigger handle into the slot at the back of the battery compartment and press it firmly into place.
6. Ensure that the main battery can be inserted into the battery compartment before securing the trigger handle in place.
7. Attach the trigger handle to the MX7 Tecton (as shown above) with the screws provided.
8. Torque the pan head screws to 3±1 in/lb (.34±.11 N/m).
9. Secure the strap tether to the trigger handle.
10. Place the stylus in the stylus holder in the bottom of the trigger handle. Tie the stylus tether to the stylus and the trigger handle.

Periodically check the trigger handle for wear and the connection for tightness. If the handle gets worn or damaged, it must be replaced. If the trigger handle connection loosens, it must be tightened or replaced before the MX7 Tecton is placed back in service.

Assembling the Carry Case

Note: Accessory installation or removal should be performed on a clean, well-lit surface. When necessary, protect the work surface, the MX7 Tecton, and components from electrostatic discharge.

The main battery can be removed and inserted without taking the MX7 Tecton out of the carry case.

1. Remove any cables connected to the I/O port at the bottom of the MX7 Tecton.
2. Remove the rubber boot from the MX7 Tecton.
3. Separate the hook and loop fabric on the carry case without removing the hook and loop fabric from the carry case.
4. Slip the removable, clear plastic protector for the keypad and touch screen into the case. Position it against the openings for the keypad and touch screen in the carry case. The voice case does not require the clear plastic protector.
5. Slide the MX7 Tecton into the case, making sure the touch screen and keypad (including the Scan LED) are visible and accessible through the front openings of the case.
6. Securely tether the stylus to the case, if necessary. Place the stylus in the stylus holder on the handstrap or in the trigger handle.
7. Loosen then tighten the handstrap (on cases without a trigger handle opening) until the carry case assembly is secure in your hand.
8. When a shoulder strap is available, secure the clips at each end of the shoulder strap to the D rings on either side of the carry case. The shoulder strap allows the MX7 Tecton to hang upside down until needed.

Carry Case with Metal Snaps

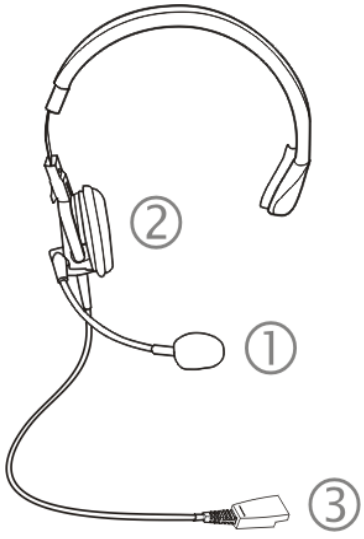
The metal snap has a bulge in the lip and a dot indentation on the opposite side. To close the carry case, tuck the lip bulge under the snap lip and press on the dot to snap closed.

Pull the snap up to open the carry case.

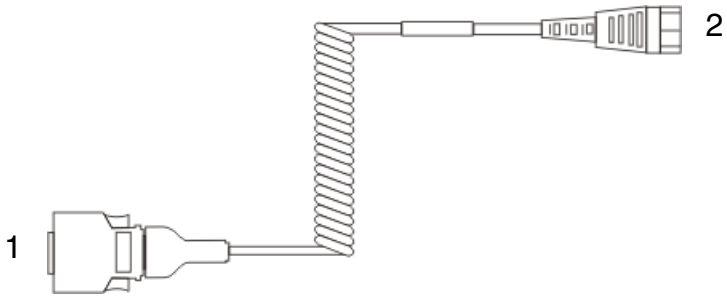
Connecting a Headset Cable

The headset consists of an earpiece, a microphone, a clothing clip and a cable. The headset attaches to the audio cable end of the voice cable which attaches to the MX7 Tecton.

When the headset is cabled to the MX7 Tecton, the microphone and speaker on the front of the device are automatically disabled.

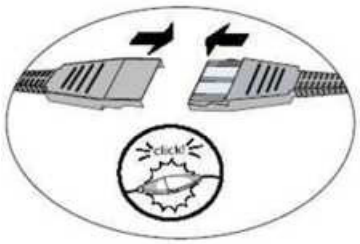


1. Microphone
2. Headphones
3. Connects to voice cable end of voice cable



Voice Cable
1. Connect to MX7 Tecton I/O port
2. Connect to Headset Cable

1. Connect the MX7 Tecton voice cable I/O connector to the I/O port on the MX7 Tecton.



2. Slide the voice cable ends of the headset assembly and the voice cable together until they click shut. Do not twist or bend the connectors.
3. Adjust the headset and microphone. Use the clothing clip to secure the cable to your clothing.

Adjusting Headset / Microphone and Securing the Cable

Do not twist the microphone boom when adjusting the microphone. The microphone should be adjusted to be about two finger widths from your mouth.

Make sure the microphone is pointed at your mouth. Note the small “Talk” label near the mouthpiece. Make sure the Talk label is in front of your mouth. The microphone cable can be routed over or under clothing.

Under Clothing

- Leave the cable exposed only at the top of the collar.
- Be sure to leave a small loop of cable to allow movement of your head.

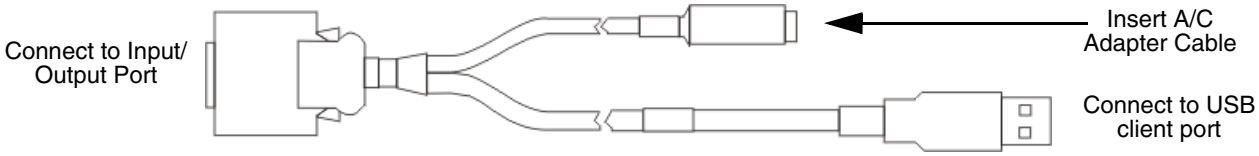
Over Clothing

- Use clothing clips to hold the cable close to your body.
- Tuck the cable under the belt, but leave a small loop where it goes under the belt.
- Do not wear the cable on the front of your body. It may get in your way or get caught on protruding objects.

Connecting the USB Client and Power Cable

Note: AC/DC Adapter must be assembled before this process begins.

Note: Do not connect AC power to the AC Adapter until instructed in the following procedure.

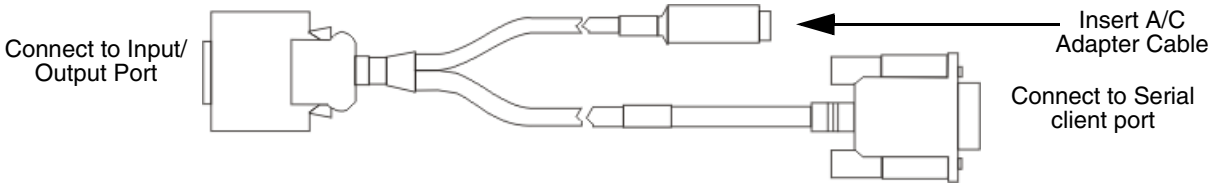


1. Holding the cable I/O connector, pinch the catch release buttons in until the catches are open. Connect the cable to the MX7 Tecton I/O port by matching the shape of the I/O connector on the cable with the shape of the I/O connector at the base of the MX7 Tecton. Release the catch release buttons.
2. Insert the AC adapter single pin cable.
3. Connect the AC Adapter to an indoor power source (wall outlet).
4. Insert the USB client plug into the target USB Client port. The MX7 Tecton and the USB client are connected.

Connecting the Serial and Power Cable

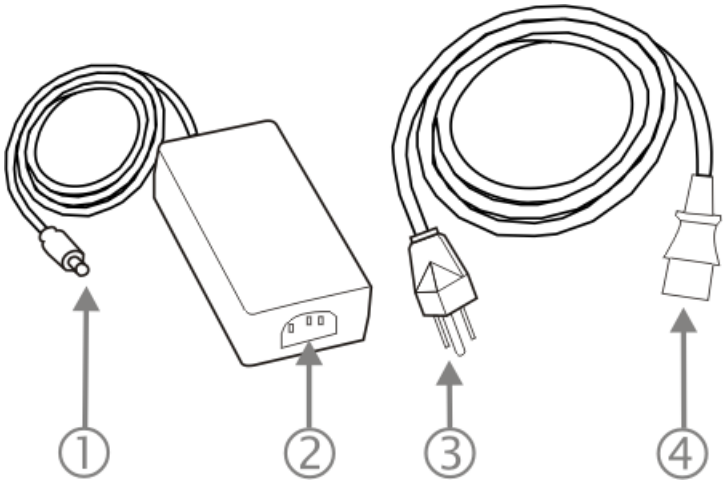
Note: AC/DC Adapter must be assembled before this procedure begins.

Note: Do not connect AC power to the AC Adapter until instructed in the following procedure.



1. Holding the cable I/O connector, squeeze the catch release buttons in until the catches are open. Connect the cable to the MX7 Tecton I/O port by matching the shape of the I/O connector on the cable with the shape of the I/O connector at the base of the MX7 Tecton. Release the catch release buttons.
2. Connect the AC adapter single pin cable.
3. Connect the assembled AC/DC Adapter to an indoor power source (wall outlet).
4. Connect the RS232 cable end to the desired serial device. Turn the thumbscrews clockwise until the connection is finger-tight. The MX7 Tecton and the serial device are connected.

Assembling the AC/DC Power Supply



1. Connects to multi-purpose cables connected to the I/O port on the MX7 Tecton
2. AC receptacle
3. Wall plug
4. AC connection from wall to adapter

To apply external power to the MX7 Tecton follow the steps below in sequence.

1. Plug the 3 prong AC adapter cable end into an indoor AC power source (e.g., wall outlet).
2. Firmly press the female end of the power cable into the male connector on the power adapter. When AC power is being supplied to the power adapter, the LED on the power adapter illuminates green. The AC adapter is ready for use.
3. Squeeze the catches of the (USB/Power or Serial/Power) I/O connector and push the cable connector into the MX7 Tecton I/O port until it clicks. The click means the connector is seated firmly.
4. Press the power cable connector pin from the AC adapter into the connector on the (USB/Power or Serial/Power) cable attached to the base of the MX7 Tecton. External power is now being supplied to the MX7 Tecton.

Whenever possible, use the AC power adapter with the MX7 Tecton to conserve the main battery power and maintain a charge in the internal battery.

Startup Help

Issue:

Can't change the date/time or adjust the volume.

Solution:

AppLock is installed and may be running in User Mode on the MX7 Tecton. AppLock user mode restricts access to the control panels.

Issue:

Touch screen is not accepting stylus taps or needs recalibration.

Solution:

If the touch screen is not accepting stylus taps, press Ctrl+Esc (Blue+Alt) to force the Start Menu to appear. Use the arrow keys to move from program to program. Press Enter to open folders or start a program e.g., Registry panel Warmboot button.

Issue:

The MX7 Tecton seems to lockup as soon as it is rebooted.

Solution:

There may be slight delays while the wireless clients connect to the network, authorization for voice-enabled applications complete, Wavelink Avalanche management of the MX7 Tecton startup completes, and Bluetooth relationships establish or re-establish. When the desktop appears or an application begins, the MX7 Tecton is ready for use.

Issue:

New MX7 Tecton main batteries don't last more than a few hours.

Solution:

New batteries must be fully charged prior to first use. Li-Ion batteries (like all batteries) gradually lose their capacity over time (in a linear fashion) and never just stop working. This is important to remember – the MX7 Tecton is always 'on' even when in the Suspend state and draws a small amount of battery power at all times.

Cold Storage Battery Life – minimum 2.5 hours while the unit is roaming, powered on with ambient temperature -10°C (14°F) or above, display backlight turned on, keypad LED backlight on, radio connected to Access Point, and scanner decoding bar codes. The Li-Ion main battery (MX7A381BATT, MX7393BATT, and MX7396BATTERY) has been designed specifically for the Cold Storage device. This 1250mAh battery has a blue label while the standard 2200mAh battery has a white (MX7A380BATT and MX7392BATT) label.

Issue:

Keep losing ActiveSync connection between my host computer and the MX7 Tecton.

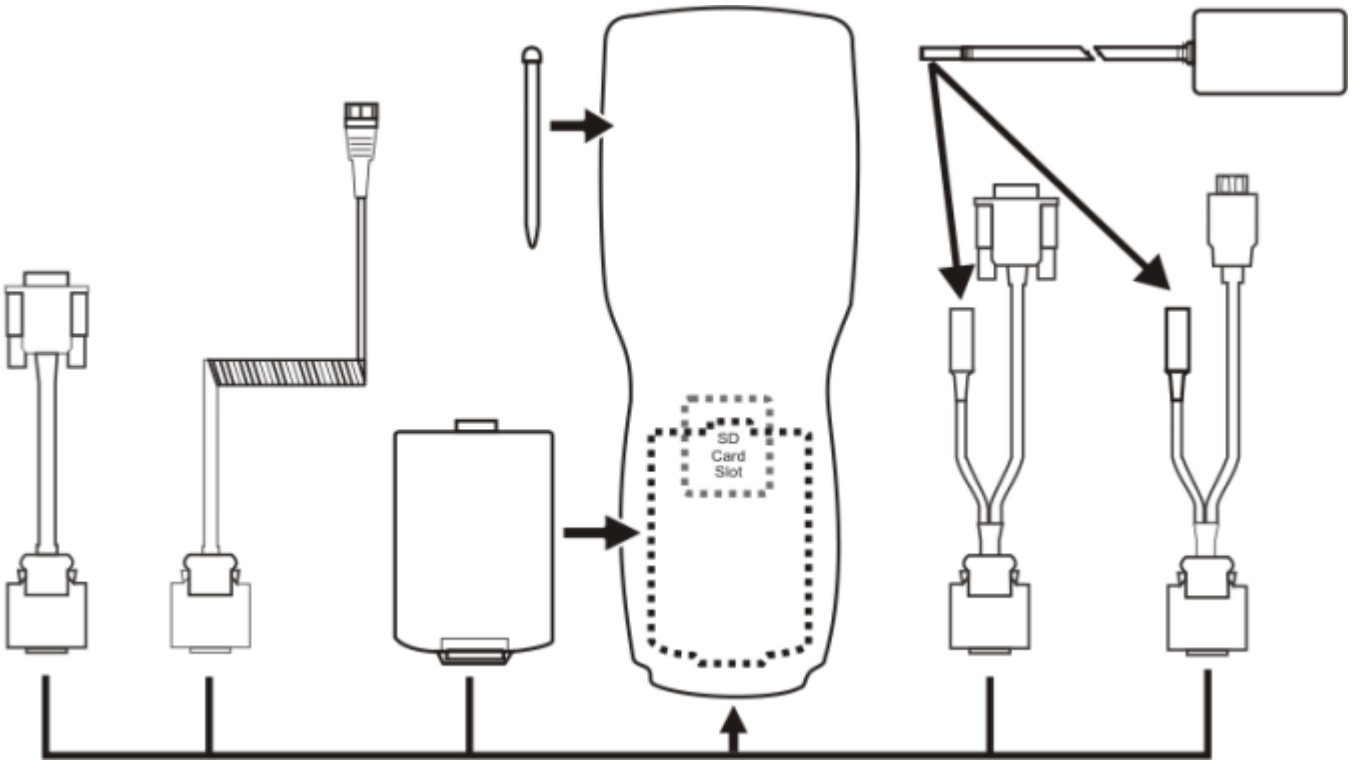
Solution:

Disconnect the USB cable, wait 1-2 seconds and reconnect the cable. The MX7 Tecton will not enter Suspend as long as an ActiveSync session is running. The ActiveSync session prevents it from going into suspend.

3

Hardware Configuration

System Hardware



802.11 a/b/g Wireless Client

The MX7 Tecton has an 802.11 network card that supports diversity with two internal antennas. The CPU board does not allow hot swapping the network card. WEP, WPA and LEAP are supported.

Central Processing Unit

The CPU is an 806MHz Marvell PXA-320 CPU. The OS image is stored in internal flash and is loaded into RAM for execution. Turbo mode switching is supported and turned on by default.

The MX7 Tecton supports the following I/O components of the core logic:

- One SD card slot under the main battery pack.
- One serial port.
- One Digitizer Input port (Touch screen).

Program CAB files, MX7 Tecton utilities, wireless drivers, the registry and registry backup information are stored in internal Flash.

System Memory

The CPU configuration supports 256MB on-board flash. The system optimizes for the amount of RAM available.

Internal flash is used for boot loader code and system low-level diagnostics code. Bootloader code is validated at system startup.

Internal SD Card Slot

One SD Memory card slot for Expansion Memory, located in the main battery well, and protected by a rubber flap. 1GB and 4GB flash memory cards are available from Honeywell.

Video Subsystem

The touch screen is a 3.5" (8.9 cm) diagonal viewing area, ¼ VGA 320 by 240 pixel TFT Reflective Active Color LCD. Backlighting is available and can be turned on and off with key sequences. The turn-off timing is configured through the **Start > Settings > Control Panel > Display** icon. The display controller supports Microsoft CE 6 graphics modes.

A touch screen allows mouse functions (tapping on the display or signature capture) using a stylus. The touch screen has an actuation force with finger less than 100 grams. The color display has an LED backlight and is optimized for indoor use.

The display appears black when the MX7 Tecton is in Suspend Mode.

Power Supply

The MX7 Tecton uses one of two batteries for operation.

- **Main Battery**. A rechargeable 2200 mAh Lithium-Ion (Li-Ion) battery pack. The battery pack recharges while in the MX7 Tecton when the device is connected to the optional external MX7 Tecton AC/DC power source. The main battery pack can be removed from the MX7 Tecton and inserted in the MX7 Tecton Battery Charger which simultaneously charges up to four battery packs in four hours. A new main battery pack can be fully charged in 6 hours when it is in an MX7 Tecton connected to AC power and 3.5 hours when it is in the MX7 Tecton battery charger.
- **Low temperature.** A rechargeable Lithium-Ion (Li-Ion) battery pack has a 1250 mAh capacity.
- **Super-capacitor (Super-cap).** No backup "battery" is used. Super-cap internal battery maintains RAM and other vital settings during a critical shutdown.

Note: An uninterrupted external power source (wall AC adapters) transfers power to the MX7 Tectons internal charging circuitry which, in turn, recharges the main battery and Super-cap battery. Frequent connection to an external power source, if feasible, is recommended to maintain main battery charge status as the Super-cap battery cannot be recharged by a dead or missing main battery.

COM Ports

The MX7 Tecton has one mini D 20-pin serial port (a multifunction I/O port) that can be configured by the user. It has a power input interface to allow powering the MX7 Tecton from an external source (AC/DC power supply or vehicle power). The power input interface range is 10 - 18VDC.

RS232 Serial Port

Configured as COM1. Bi-directional full duplex and supports data rates up to 115 Kb/s. The port does not have RI or CD signals nor does it support 5V switchable power on pin 9 for tethered scanners. The serial port driver supports full duplex communications over the serial port. It supports data exchange via ActiveSync, but does not automatically start ActiveSync when connected. The *Cable, Multipurpose RS232 and Power* and the *Adapter, RS232 PC port to D9* male accessories can be used with the RS232 serial port. External AC power is available when the multipurpose RS232/Power cable is connected. External AC power is not available for the *Adapter, RS232 PC port to D9 male* option. Power is drawn from the main battery pack when this adapter is connected..

USB Client Port

The MX7 Tecton has one USB Client port for ActiveSync applications. An accessory USB cable, Cable, Multipurpose USB and Power is available to connect the MX7 Tecton to a USB Type A plug on a PC for ActiveSync functions. External AC power is available when the multipurpose USB Client/Power cable is connected.

Audio Connection

An audio headset interface is available using the *Adapter, Audio accessory* with the I/O port. The connection cable connects the MX7 Tecton to a Voxware quick disconnect 4-pin interface. This cable adapts to specific styles of headsets for voice input, stereo or mono output. The MX7 Tecton with a Summit Client supports mono only. A 3-wire connector with (at a minimum) connections for ground, microphone, and 1 speaker. Connecting the headset to the MX7 Tecton COM port turns off audio output to the MX7 Tecton speaker on the front of the device. All sounds previously directed to the speaker are redirected to the headphone, including beeps. Bias voltage for an electric condenser microphone is available. External AC power is not available for this option. Power is drawn from the main battery pack.

Audio Support

Speaker

The speaker supplies audible verification signals normally used by the Windows operating system. The speaker is located on the front of the MX7 Tecton, above the MX7 Tecton logo. The mobile device emits a Sound Pressure Level (loudness) of at least 102 dB measured as follows:

- Frequency: 2650 + 100 Hz
- Distance: 10 cm on axis in front of Speaker opening in front of unit.
- Duration: Continuous 2650 Hz tone.

The default is 1 beep for a good scan and 2 beeps for a bad scan.

Volume Control

Volume control is managed by a Windows control panel, an API and the Orange-Scan up/down arrow key sequence.

Voice

All Microsoft-supplied audio codecs are included in the OS image. The hardware codecs, the input and output analog voice circuitry and the system design are designed to support voice applications using a headset connected to the *Adapter, Audio* accessory cable and the MX7 Tecton I/O connector.

Scanner / Imager Port

The MX7 Tecton has one integrated bar code scanner/imager port. Only one scan engine is installed at a time. Scan engines are not “hot swappable”. The MX7 Tecton may have one of the following bar code decoding engines:

- Short Range Laser Scanner, SE955I
- Base Laser Scanner, SE955E
- Multi-Range “LORAX” Laser, SE1524ER
- Hand Held Products 2D Area Imager, 5300
- Honeywell Laser Scanner, N43XX
- Honeywell Laser Scanner, N73XX

Note: 955E does not support aim mode. Any attempt to adjust the aiming beam using 955E programming bar codes will fail. The Base Laser scanner does not decode Codablock, Code93i or Telepen symbologies.

The integrated scan engine activates when the Scan button on the front of the MX7 Tecton is depressed or when the trigger on an installed trigger handle is depressed. The Data Collection application is available to set scanner/imager options.

Functionality of the integrated scan engine driver is based on the decoder driver version installed in the MX7 Tecton. Functions may include audible tones on good scan (at the maximum dB supported by the speaker), failed scan, Scan LED indication of a scan in progress, among other functions. If enabled, a vibration device provides a tactile response on a good scan event.

Bluetooth EZPair (or LXEZ Pairing)

The MX7 Tecton contains Bluetooth version 2.1 with Enhanced Data Rate (EDR). Bluetooth device connection (or pairing) can occur at distances up to 32.8 ft (10 meters) Line of Sight. The wireless client retains network connectivity while Bluetooth is active and the paired device is within range.

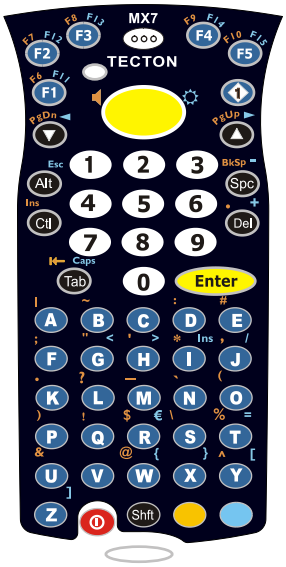
The user will not be able to select PIN authentication or encryption on connections from the MX7 Tecton. However, the MX7 Tecton supports authentication requests from pairing devices. If a pairing device requests authentication or encryption, the MX7 Tecton displays a prompt for the PIN or passcode. Maximum encryption is 128 bit. Encryption is based on the length of the user’s passcode.

Bluetooth devices can be paired and managed using the EZPair (or LXEZ Pairing) control panel.

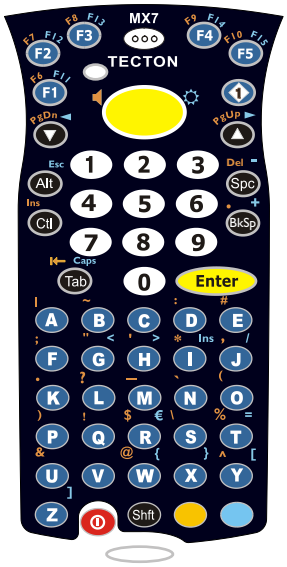
- The MX7 Tecton does not have a Bluetooth managed LED.
- The LED on a mobile Bluetooth scanner illuminates during a scanning operation; the Scan LED on the MX7 Tecton does not illuminate.
- Bar code data captured by a mobile Bluetooth scanner is manipulated by the settings in the Data Collection control panel.
- Multiple beeps may be heard during a bar code scan using a mobile Bluetooth scanner; beeps from the mobile Bluetooth scanner as the bar code data is accepted/rejected, and other beeps from the MX7 Tecton during final bar code data manipulation.

Keypads

55 Key Keypads



ANSI Primary Delete



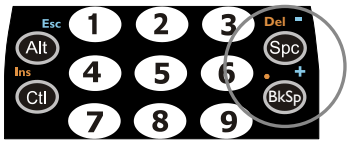
ANSI Primary Backspace

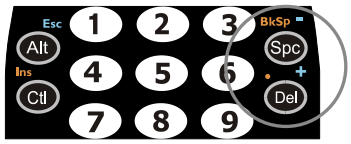
5250 Primary Delete

Using the 55 Key Alpha-Numeric Keypad

There are three options available for the 55 key keypad:

1. 55 key Alphanumeric Keymap - Primary Delete (page 12-1).
2. 55 Key 5250 Alphanumeric KeyMap - Primary Delete (page 12-6). 5250 commands are displayed on the keypad overlay next to the affected keys.
3. 55 key Alphanumeric Keymap - Primary Backspace (page 12-11). This keypad resembles the ANSI Primary Delete keypad with the exception that the Del key function on the ANSI Primary Delete keypad is replaced by the BkSp key function.





- When using a sequence of keys that includes a sticky key, press the sticky key first, release it, then press the rest of the key sequence.
- When using a sequence of keys that includes the Orange or Blue keys, press the color key first then the rest of the key sequence.
- Alphabetic keys default to lower case letters. Press the Shft key, then the alphabetic key for an uppercase letter.
- When the computer boots, the default condition of Caps (or CapsLock) is Off. The Caps (or CapsLock) condition can be toggled with Blue plus Tab key sequence.

32 Key Keypad

Triple Tap Alpha

Using the 32 Key Numeric with Triple Tap Alpha

32 key Numeric-Alpha Keymap (page 12-16)

- When using a sequence of keys that require an alpha key, first press the Alph key. Use the Shft sticky key or the Caps key sequence (Blue+Tab) for upper case alphabetic characters. See 32 key Numeric-Alpha Keymap (page 12-16).
- Pressing the Alph key forces “Alpha” mode for the 2,3,4,5,6,7,8, and 9 keys. The 1 and 0 keys continue to place a 1 and 0 into the text field.
- To create a combination of numbers and letters before pressing Enter, tap the Alph key to toggle between Alpha and Numeric mode.
- When using a sequence of keys that do not include the Alph key but does include a sticky key, press the sticky key first then the rest of the key sequence.

Display

The touch screen display is an active color LCD unit capable of supporting VGA graphics modes. Display size is 240 x 320 pixels in portrait orientation. The covering is designed to resist stains. The touch screen allows signature capture and touch input. A pen stylus is included. The touch screen responds to an actuation force (touch) of 4 oz. of pressure (or greater). The color display is optimized for indoor lighting. The display is black when the device is in Suspend Mode or when both batteries have expired and the unit is Off.

Display Backlight Timer

When the Backlight Timer expires the display backlight is turned off. The default value for the battery power timer is 3 seconds. The default value for the external power timer is “never” and the check box is blank. The backlight timer dims the backlight on the touch screen and the keypad at the end of the specified time. When the display wakes up, the Backlight timer begins the countdown again. The keypad backlight can be synchronized with the display backlight activity.

Status LEDs

- The MX7 Tecton does not have a Bluetooth managed LED. Bluetooth activity indicators are located in the taskbar.
- System Status LED is located at the top left of the keypad, above the Scan button.
- The Scan Status LED is located below the keypad.
- The Alpha Mode LED is located below the F4 key on the 32-key keypad (Numeric-Alpha keypad).

LED	Color - Activity	Indicates ...
System Status	Red - Blinking	Power fail. Replace the main battery with a fully charged main battery. Or Connect the MX7 Tecton to external AC power then replace the main battery with a fully charged main battery.
	Red - Steady	Main Battery Low. If the main battery is not replaced with a fully charged battery before the main battery fails, the MX7 Tecton is turned Off.
	Green - Blinking	Display Off. No user intervention required.
	No Color	MX7 Tecton is either full on - with the display on (backlights may be dimmed when the status LED has no color) or in Suspend - with the display off.
Scan Status	Green - Steady	Good scan.
	Red – Steady	Scan in progress.
	No color	Integrated Scanner / Imager ready for use.
	Amber - Steady	Bar code decoder engine is storing changed parameters.
Alpha Mode (Alph LED)	Green - Steady	MX7 Tecton 32-key is in Alpha character input mode.
	No color	MX7 Tecton 32-key is in Numeric key input mode.

Cold Storage Configuration

- MX7 Tecton 1250mAh Cold Storage battery has a blue label.
- Snowflake decal above the MX7 Tecton keypad.
- Heating element visible on the touch screen and the scan aperture.

Cold storage battery is recharged in the MX7 Tecton Battery Charger, MX7 Tecton Desk Cradle and when in an MX7 Tecton attached to an external power source (e.g., AC adapter).

The Cold Storage version is designed to operate normally when reading bar codes and moving from, and into, cold storage warehouses, freezers and vehicles where the temperatures may vary between -30°C and 5°C (-22°F and 41°F).

Cold Storage Battery

There is no change in the way the Cold Storage battery is inserted into and removed from the MX7 Tecton battery well.

Battery Life – minimum 2.5 hours while the unit is roaming, powered on with ambient temperature -10°C (14°F) or above, Display backlight turned on, Keypad LED backlight on, radio connected to Access Point, and scanner decoding bar codes.

The Li-Ion main battery (MX7A381BATT and MX7393BATT) has been designed specifically for the Cold Storage device. This 1250mAh battery has a blue label while the standard MX7 Tecton 2200mAh battery has a white (MX7A380BATT and MX7392BATT) label.

Snowflake Decal

A Cold Storage device has a snowflake decal between the touch screen and the keypad. The decal is located to the left when the screen is facing forward.

Heating Elements

Heating elements activate when ambient temperature drops below 0°C (32°F). Using the stylus when performing screen touch functions is recommended. There may be some condensation as the Cold Storage device moves in and out of cold storage areas. The condensation on the touch screen and the scan aperture quickly dissipates.

The touch screen heating elements and scanner aperture heating elements may be visible when the Cold Storage device is tilted slightly. No user interaction is required to turn the heating elements on/off. Stylus taps on the touch screen function normally. Due to the heating element overlaying the scan aperture, bar code scanning may require the user to move the scan aperture closer to the bar code for good scan results.

Recharging Cold Storage Batteries

The Cold Storage battery pack can be recharged to full capacity while in a Cold Storage MX7 Tecton connected to an external power source and also while the Cold Storage battery pack is inserted in the charging bay in a powered MX7 Tecton cradle. The battery pack temperature must be above 10°C (50°F) before re-charging can begin.

Battery packs in the Battery Charger begin charging when the battery pack temperature is between 10°C (50°F) and 40°C (100°F).

To charge the Cold Storage battery pack to full capacity, the Battery Charger firmware must be V1.07 or greater. The firmware version is noted on the battery charger label on the bottom of the charger.

Contact *Product Service and Repair* (page 16-1) if your battery charger firmware needs to be upgraded.

The Battery Charger and AC adapter are not designed to operate in a freezer or cold storage environment.

Hot-swapping the Cold Storage Battery

The Cold Storage mobile device, with a fully charged Super-cap battery, retains data during a main battery hot-swap at -30°C (-22°F) for at least 90 seconds. The temperature of the fully charged replacement Cold Storage main battery must be +10°C (14°F), or above.

Normal Operation Temperature Ranges

- In the freezer where the temperature ranges between –30°C to -18°C (-22°F to 0°F).
- In the loading dock where temperature ranges between 0°C to 5°C (32°F to 41°F) with the relative humidity at 65%
- Moving between the freezer and a loading/unloading area where the temperature transitions from -30°C to 5°C (-22°F to 41°F).

4

Power Modes and Batteries

Power Modes

The MX7 Tecton has three power modes: On, Suspend and Off.

On Mode

The Display

When the display is On:

- the keypad, touch screen and all peripherals function normally
- the display backlight is on until the Backlight timer expires

The MX7 Tecton

After a new MX7 Tecton has been received, a charged main battery inserted, and the Power key tapped, the MX7 Tecton is always On until both batteries are drained completely of power.

When the main battery and Super-cap battery are drained completely, the unit is in the Off mode. The unit transitions from the Off mode to the On mode when a charged main battery is inserted or external power is applied and the Power key is pressed.

Suspend Mode

The Suspend mode is entered when the unit is inactive for a predetermined period of time or the user taps the Power key. MX7 Tecton Suspend timers are set using Windows control panels.

Wake-up Events - all configurable via a Power Management API call:

- Any key on the keypad
- Stylus touch on the touch screen
- Handle trigger press
- Connecting to AC adapter
- Power button tap
- USB connection
- COM port control CTS
- Real time clock
- Bluetooth device reconnect / disconnect message

When the MX7 Tecton wakes up, the Display Backlight and the Power Off timers begin the countdown again. When any one of the above events occurs prior to the Power Off timer expiring, the timer starts the countdown again. The MX7 Tecton does not need to be placed in Suspend mode before hotswapping the main battery.

Off Mode

The unit is in Off Mode when the main battery and the Super-cap battery are depleted. Insert a fully charged main battery and press the Power key to turn the MX7 Tecton On.

Batteries

The MX7 Tecton is designed to work with a Lithium-Ion (Li-ion) battery. Under normal conditions it should last approximately eight to ten hours before requiring a recharge. The more you use the scanner or the wireless transmitter, the shorter the time required between battery recharges.

A suspended MX7 Tecton maintains settings for a minimum of two days using a main battery that has reached the Low Warning point and a fully charged Super-cap internal battery. The MX7 Tecton retains data, during a main battery hot swap, for at least 5 minutes.

Note: New main battery packs must be charged prior to use. This process takes up to four hours in an MX7 Tecton Battery Charger and six hours when the MX7 Tecton is connected to external power.

Checking Battery Status

Tap the Battery tab on the Power panel. Battery level, power status and charge remaining is displayed.

Note: When the Battery control panel is displayed power management is disabled, meaning the backlights and display will not turn off nor will the unit suspend, after the configured inactivity times expire.

Main Battery Pack

The main battery pack has a rugged plastic enclosure that is designed to withstand the ordinary rigors of an industrial environment. Exercise care when transporting the battery pack making sure it does not come in contact with excessive heat or any power source other than the MX7 Tecton Battery Charger or the MX7 Tecton unit.

When the main battery pack is properly installed in the unit it provides up to eight hours of operation depending upon use and accessories installed. The battery pack is resistant to impact damage and falls of up to four feet to a concrete surface. Under normal conditions it should last approximately eight hours before requiring a recharge. The more you use the scanner or the wireless transmitter, the shorter the time required between battery recharges.

Battery Hotswapping

Note: When the internal battery power is Low or Very Low (can be viewed on the Power control panel) connect the AC adapter to the MX7 Tecton before replacing the main battery pack.

When the main battery power level is low, the MX7 Tecton will signal the user with the low battery warning indicator (the Status LED remains a steady red) that continues until the main battery is replaced, the battery completely depletes, or external power is applied to the MX7 Tecton using an AC Adapter.

You can replace the main battery by first placing the MX7 Tecton in Suspend Mode then removing the discharged main battery and installing a charged main battery within a five minute time limit (or before the Super-cap internal battery depletes). When the main battery is removed the MX7 Tecton enters Critical Suspend state; the MX7 Tecton remains in Suspend mode, the display is turned off and the internal battery continues to power the unit for at least five minutes.

Though data is retained, the MX7 Tecton cannot be used until a charged main battery is installed. After installing the new battery, press the Power key. Full operational recovery from Suspend can take several seconds while the client is re-establishing a network link. If the internal battery depletes before a fully charged main battery can be inserted, the MX7 Tecton will turn Off.

Low Battery Warning

It is recommended that the main battery pack be removed and replaced when its energy depletes. When the main battery Low Battery Warning appears (the Status LED remains a steady red) perform an orderly shut down, minimizing the operation of any installed devices and insuring any information is saved that should be saved.

Super-cap Internal Battery

The MX7 Tecton has an internal battery that is designed to provide limited-duration electrical power in the event of main battery failure. The energy needed to maintain the internal battery near full charge at all times is drawn from the MX7 Tecton main battery. It takes 5 minutes or less to fully charge the internal battery. The duration of internal battery life is dependent upon operation of the MX7 Tecton, its features and any operating applications. The internal battery has a minimum service life of two years. The Super-cap internal battery is replaced by Honeywell.

Handling Batteries Safely

- Never dispose of a battery in a fire. This may cause an explosion.
- Do not replace individual cells in a battery pack.
- Do not attempt to pry open the battery pack shell.
- Be careful when handling any battery. If a battery is broken or shows signs of leakage do not attempt to charge it. Dispose of it using proper procedures.

Caution

Nickel-based cells contain a chemical solution which burns skin, eyes, etc. Leakage from cells is the only possible way for such exposure to occur. In this event, rinse the affected area thoroughly with water. If the solution contacts the eyes, get immediate medical attention.

NiMH and Li-Ion batteries are capable of delivering high currents when accidentally shorted. Accidental shorting can occur when contact is made with jewelry, metal surfaces, conductive tools, etc., making the objects very hot. Never place a battery in a pocket or case with keys, coins, or other metal objects.

5 Software Configuration

Introduction

There are several different aspects to the setup and configuration of the MX7 Tecton. Many of the setup and configuration settings are dependent upon the optional features such as hardware and software installed on the mobile device. The examples found in this section are to be used as examples only, because the configuration of your specific MX7 Tecton may vary. The following sections provide a general reference for the configuration of the MX7 Tecton and some of its optional features. Contact *Technical Assistance* (page 16-1) for information on the latest upgrades.

Windows Mobile

Note: For general use instruction, refer to commercially available Windows Mobile user's guides or the Windows Mobile on-line Help application in the MX7 Tecton

This section's contents assumes the system administrator is familiar with Microsoft Windows options and capabilities loaded on most standard Windows desktop computers.

Therefore, the sections that follow describe only those Windows capabilities that are unique to the MX7 Tecton and its Windows Mobile environment.

Installed Software

Note: Some options require an external modem connection. Modems are not available from Honeywell.

When you order an MX7 Tecton you receive the software files required by the separate programs needed for operation and wireless client communication. The files are loaded and stored in folders in the mobile device.

This section lists the contents of the folders and the general function of the files. Files installed in each MX7 Tecton are specific to the intended function of the MX7 Tecton.

Files installed in mobile devices that are configured for a wireless environment usually contain a radio specific driver – the driver for the radio is specific to the manufacturer of the radio installed in the wireless host environment and is not interchangeable.

Software Load

The software loaded on the MX7 Tecton computer consists of Windows Mobile Operating System, hardware-specific OEM Adaptation Layer, device drivers, Internet Explorer for Windows Mobile browser and MX7 Tecton-specific utilities. The software supported by the MX7 Tecton is summarized below:

- Operating System - Full Operating System License: Includes all operating system components, including Windows Mobile kernel, file system, communications, connectivity (for remote APIs), device drivers, events and messaging, graphics, keyboard and touch screen input, window management, and common controls.
- Network and Device Drivers
- Bluetooth (Option)
- AppLock (Option)
- RFTerm (VT220, TN5250, TN3270) Terminal Emulation (Option).
- CE API Routines

Software Backup

Application programs and data that are normally RAM resident are backed up via ActiveSync.

Version Control

Version numbers are applied to the boot loader and the OS image independently. The version information stored consists of the build number, plus the date and time of compile (in lieu of a build number). These version numbers are stored in non-volatile storage, where the user cannot inadvertently modify them. A Settings panel and API are provided so the user can reference the version numbers for support purposes.

The MX7 Tecton has a unique 128-bit ID code as required by the Windows Mobile specification. This ID number is generated by the boot loader. This ID code is available in the About Info settings panel, and via a Win32 standard API.

In addition, an API is provided to return a standard copyright string, so that applications may reference this to be sure they are running on a Honeywell mobile device for licensing purposes.

Boot Loader

The MX7 Tecton supports a proprietary boot loader. It is the responsibility of the boot loader to:

- Initialize all system hardware
- Initiate OS startup
- Handle wakeup from system suspend, loading saved state

The MX7 Tecton re-starts the OS during warmboot and restart.

Startup Folders and Launch Sequences

The MX7 Tecton operating system uses two startup folders:

- User applications placed in the Windows\Startup folder automatically run during a reboot. They are deleted upon a clean boot.
- User applications placed in the System folder automatically run during a reboot.

Software Development

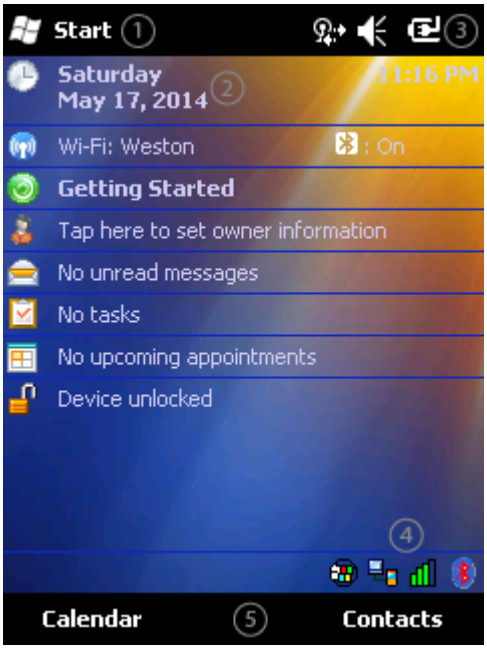
The *CE API Programming Guide* documents CE API calls for the MX7 Tecton. It is intended as an addition to the standard Microsoft Windows Mobile API documentation.

A Software Developers Kit (SDK) and additional information about software development can be found on the Developer Portal. Contact *Technical Assistance* (page 16-1) for more information.

Today Screen

For general use instruction, refer to commercially available Windows Mobile user guides or the Windows Mobile on-line Help on the MX7 Tecton.

The main screen for the MX7 Tecton is known as the Today screen. The Today screen shows various options and status icons. The Today screen appearance can be configured using the Today (page 5-22) control panel. Both the appearance of the Today screen and the items displayed may be configured.



1. Start menu
2. Configurable Today screen listing
3. Notification Bar
4. Status icons
5. Soft Keys

Start Menu

The Start menu consists of applications and folders.

- Selecting an application from the menu starts that application.
- Selecting a folder opens a window displaying the contents of the folder.
- Selecting Settings displays the Settings panels by category.
- Selecting Help displays context sensitive help. The contents displayed in the help window vary depending on the screen displayed before Help was accessed.

Programs not appearing on the Start menu can be accessed by using the File Explorer.

Configurable Today Screen Listing

The items displayed in the Today screen listing can be configured from **Start > Settings > Today > Items**. For more information, see Today (page 5-22) settings later in this chapter.

Date

When the Date is enabled to display on the Today screen, the date is displayed on the left side of the screen and the time is displayed on the right side. If there are any alarms set, a bell icon is displayed under the current time. For more information, see the Clock & Alarms (page 5-14).

Device Unlocked / Device Locked

When the MX7 Tecton is unlocked, tapping on **Device unlocked** locks the MX7 Tecton.

When the MX7 Tecton is locked, tapping on **Unlock** at the bottom of the screen unlocks the MX7 Tecton. Depending on the settings, a password may be required. The MX7 Tecton can also be configured to lock after a period of inactivity. For more information, see the Lock (page 5-16) settings.

Notification Bar

The Notification Bar is displayed at the top of the Today screen. The notification bar remains visible even when other screens are selected, though the icons displayed may vary.

When the Notification bar is displayed on other screens there may be an X (close the current screen/program) or an ok (accept the current input and close the screen).

Category	Icon	Function
Network		The Windows Mobile Wireless Manager is managing the wireless connection and the MX7 Tecton is connected to a wireless network.
Network		A wireless manager is managing the wireless connection.
Network		A wireless manager is managing the wireless connection and has detected one or more wireless networks in range.
Network		A wireless manager is managing the wireless connection and has not detected a wireless network in range.
Volume		The speaker is on.
Volume		The speaker is off.
Volume		Vibrate is on.
Power		The MX7 Tecton is connected to external power.
Power		The MX7 Tecton is operating on battery power. The strength of the battery is indicated by the number of bars displayed: 0 (low battery) to 4 (fully charged battery).

Status Icons

Additional icons may be displayed at the lower edge of the Today screen.

Note: Summit signal strength icons are displayed only when the Summit Client Utility is controlling the radio.

Icon	Function
	MX7 Tecton is connected to one or more of the targeted Bluetooth device(s).
	MX7 Tecton is not connected to any Bluetooth device. MX7 Tecton is ready to connect with any Bluetooth device. MX7 Tecton is out of range of all paired Bluetooth device(s). Connection is inactive.
	Summit radio is not currently associated or authenticated to an Access Point.
	The signal strength for the currently associated/authenticated Access Point is less than -90 dBm
	The signal strength for the currently associated/authenticated Access Point is -71 dBm to -90 dBm
	The signal strength for the currently associated/authenticated Access Point is -51 dBm to -70 dBm
	The signal strength for the currently associated/authenticated Access Point is greater than -50 dBm

More information on Bluetooth activity and settings can be found in Bluetooth Configuration (page 7-1).

Soft Keys

Soft Keys are displayed at the bottom of the Today screen. The keys displayed vary by the active screen/application.

The soft keys generally provide menus for the selected application. By default, on the Today screen, the left Soft Key (Calendar) can also be accessed by pressing F1 and the right Soft Key (Contacts) can be accessed by pressing F2. The assignments for the Soft Keys can be edited using Buttons (page 5-24).

Installed Programs

Additional information on installed programs is listed below.

Internet Explorer Mobile

This browser is a subset of and is compatible with IE 7.0 (as might be installed on a desktop PC). Internet Explorer Mobile 8 has two viewing modes: Reading mode and Overview mode.

For information on general configuration options, see the Windows Mobile help system on the MX7 Tecton or other commercially available Internet Explorer configuration resources. Tap the IE Menu soft key (on the lower right) and select **Tools > Options** to set up the default home page, view browsing history, setup privacy and security, preferred language, and Other options.

If an Internet Explorer webpage is larger than the MX7 Tecton screen can display at one time, use touch screen gestures for horizontal and vertical scrolling.

For information on the version of Internet Explorer loaded on the MX7 Tecton, tap the Favorites soft key and select About Internet Explorer.

Office Mobile Applications

Office 2003 and Office 2007 formats are supported, though these are subset applications so not all objects may appear as expected.

ActiveSync handles all file format conversions for Office Mobile files transferred between the MX7 Tecton and the host PC.

ActiveSync

ActiveSync can be setup to synchronize with an Exchange server. Contact your system administrator for configuration information.

AppLock (Option)

The AppLock program is accessed by the user or the AppLock Administrator at bootup or upon completion of a cold boot. Set parameters using the Administration option in the Settings Panel.

Summit

SCU (Summit Client Utility)

Summit automatically installs and runs after every cold boot. See Wireless Network Configuration (page 11-1) for Summit Client Utility setup information and instruction.

Certs

Contents of README.TXT file located in **Start > Summit > Certs** menu option. See Wireless Network Configuration for instruction on acquiring CA and user certificate files.

Windows Media

Codecs are included for WMA, WMV, MP3 and WAV files.

Bluetooth (Option)

Only installed on a Bluetooth equipped MX7 Tecton. The System Administrator can Discover and Pair targeted Bluetooth devices for each MX7 Tecton. The System Administrator can enable / disable Bluetooth settings and assign a Computer Friendly Name for each MX7 Tecton. Bluetooth can be accessed using the Bluetooth control panel, or by tapping the Bluetooth icon on the Today screen.

RFTerm (Option)

The application can be accessed by tapping **Start > RFTerm**.

Refer to the *RFTerm Reference Guide* for complete information and instruction. WAV files added by the user should be stored in System\LXE\RFTerm\Sounds.

Status Popup

The Status Popup provides real time information on several status icons when a specified keypress occurs.

To use the Status Popup, first map a key to the Status window. Use the Buttons panel (**Start > Settings > Personal > Buttons**) to assign a key to Admin Statpop (for the Admin Popup) and StatPopup (for the User Popup). Use a Diamond key for the popup. If a Function key is used, that Function key is not available to other applications such as RFTerm.

Use the MX7 Tecton Options control panel to configure other parameters including:

- Dismiss Status Popup on 5 second timeout.
- Information to include in Admin or User Status Popup.

The Status Popup can be dismissed by the expiration of the timeout (if enabled), tapping the status window or pressing the key assigned to close the popup.

For more information, refer to the Buttons (page 5-24) and MX7 Tecton Options (page 5-40)settings.

HSM Connect (or LXEConnect)

HSMConnect allows a user with an ActiveSync connection between a PC and the MX7 Tecton to display the MX7 Tecton screen on the host PC. Any keystrokes on the host PC are passed to the MX7 Tecton as if they were keystrokes on the MX7 Tecton keypad.

HSM Connect for the MX7 Tecton running Windows Mobile is available for download to the MX7 Tecton from the *Getting Started Disc.* Contact Technical Assistance (page 16-1) if the *Getting Started Disc* shipped with the MX7 Tecton is not available.

GrabTime

GrabTime is a utility to synchronize the MX7 Tecton with a world-wide time server. GrabTime can be started as a service by setting it in the Launch option. See Enhanced Launch Utility (page 9-1) for information.

Synchronize with a local time server

- Use ActiveSync to copy GrabTime.ini from the **My Device > Windows** folder on the MX7 Tecton to the host PC.
- Edit GrabTime.ini (on the host PC) to add the local time server's domain name to the beginning of the list of servers. You can then optionally delete the remainder of the list.
- Copy the modified GrabTime.ini to the **My Device > Windows** folder on the MX7 Tecton.

Enhanced Launch

Launch is a utility that runs automatically at startup. A partial list of Enhanced Launch functions includes:

- Launch a .CAB file
- Run an .EXE or .BAT file
- Process a .REG file
- Manipulate files and directories
- Modify registry keys
- Perform conditional operations

Note: The Enhanced Launch utility does not interact with or affect the AppLock Launch command.

For a complete list of Launch functions including commands and command structure, see Enhanced Launch Utility (page 9-1).

MX7 Tecton OS Upgrade

Depending on the size of the operating system, the total time required for a successful upgrade may require several minutes.

The OS upgrade files are unique to your MX7 Tecton physical configuration and date of manufacture. OS upgrade files designed for one device configuration should not be used on a different device configuration.

The MX7 Tecton running Windows Mobile must be returned to the manufacturer, Honeywell, if the device is to be re-imaged with any other Windows operating system (for example, Windows CE 6).

During the upgrade process all settings revert to factory defaults. Parameters will need to be changed from factory defaults to your preferred values at the conclusion of the upgrade process.

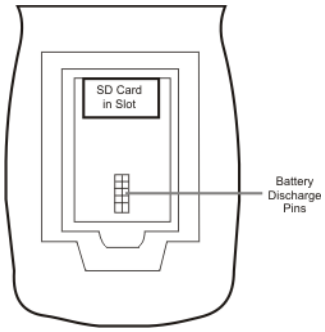
Preparation

- Contact Technical Assistance (page 16-1) to get the OS upgrade files from Honeywell.
- Removing and installing the SD Flash card should be performed on a clean, well-lit surface.
- Always perform MX7 Tecton updates when it has a fully charged main battery and/or a dependable external power source connected to the MX7 Tecton.

Procedure

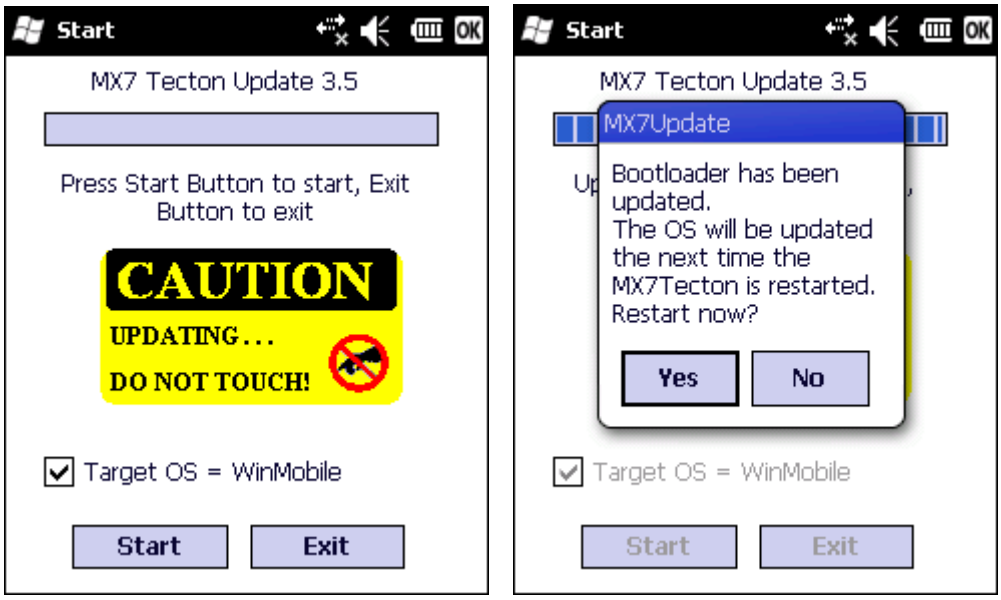
1. Place the new image files and MX7Update on a SD card.
2. Place the MX7 Tecton in Suspend Mode and remove the main battery.

SD Card Location



Update Icon

3. Lift the rubber barrier and slide the SD card out of the slot. Do not remove the rubber barrier. The MX7 Tecton may not have a SD card in the slot because the OS is in flash.
4. Place the card with the new image files on it into the SD slot. The label on the SD card should be facing up.
5. Launch MX7UPDATE.EXE in **My Device > Storage Card**.
6. Verify the Target OS = WinMobile check box is checked
7. **Important:** If a failure occurs during the update, DO NOT RESTART (or coldboot). Follow the instructions on the screen to Exit the update utility then restart the update utility.
8. Tap Start to start the update. The check box is dimmed when the Update is processing. Do not touch the device until the install/update is complete.



When the bootloader process is complete, tap the Yes button to reboot to complete the update process. Tap the No button and the update is not complete.

When the process is finished (MX7 Tecton has restarted), remove the SD card, replace the rubber barrier and replace the main battery. Turn the MX7 Tecton on.

Check the OS update version by viewing the **About Info** (or **About LXE**) Settings panel.

Note: If the application displays "Update OS Image Failed" or "Update Boot Loader Image Failed", do not Restart the system manually. Perform a warm boot, then try the upgrade again. Restarting will cause a system crash, since there is no valid image in the MX7 Tecton system.

Battery State and OS Upgrade

A fully charged main battery should be installed in the MX7 Tecton prior to upgrading the operating system. A prompt may appear when the battery reaches Critical Low that informs the user there is not enough power in the main battery to perform the upgrade.

The operating system will not be able to execute the OS upgrade when the battery level is too low (25% or less), as there is a high risk that the power remaining in the battery expires when executing the upgrade and the MX7 Tecton will be left in an inoperable state.

When main battery power level is too low, connect external power to the MX7 Tecton before performing the upgrade procedure. Do not disconnect external power before the upgrade process is complete.

The MX7 Tecton running Windows Mobile must be returned to Honeywell if the device is to be imaged with any other Windows operating system (for example, Windows CE).

Update Help

Issue:

The powered device won't boot up after the upgrade is finished.

Solution:

Send the MX7 Tecton to Product Service and Repair (page 16-1) for re-imaging. ***Warning:*** Opening the device e.g., removing endcaps or access panels, etc., could void the user's authority to operate this equipment.

Start Menu Options

The following options represent the factory default program installation. Your system may be different based on the software and hardware options purchased.

Use the up and down arrow keys on the MX7 Tecton to quickly scroll through the icons,

or,

using screen touch gestures, brush the window up or down with a finger or the stylus.

ActiveSync. Basic ActiveSync configuration, including synchronization with an Exchange server. See Using ActiveSync (page 5-70)

Avalanche. Enabler Installation and Configuration (page 10-1) installation files are loaded, but not installed at initial startup, on the mobile device when it is shipped.

Calculator (page 5-54)

Calendar (page 5-55). Can be synchronized with PC Outlook calendar using ActiveSync.

Contacts (page 5-55). Address book application. Can be synchronized with PC Outlook address book using ActiveSync.

Email (page 5-56). Can be synchronized with PC Outlook email using ActiveSync or it can synchronize with an Exchange server.

File Explorer (page 5-56). Displays a structured picture of files on the system.

Help (page 5-57). Access Windows Mobile help system on the MX7 Tecton. Options to search using Windows Live Search are available.

Internet Explorer Mobile (page 5-61). Access web pages on the Internet.

Windows Live (page 5-59). Instant Messaging service. Internet access required.

Notes (page 5-58). Notebook application. Select **Menu > View Recording** Toolbar to create an audio note. Can be synchronized with PC Outlook notes using ActiveSync.

Office Mobile (page 5-11). Access to Excel, PowerPoint, Word and OneNote. Compatible with Microsoft Office 2007.

Pictures and Video (page 5-58). Picture/video viewer application. Can be synchronized with PC My Documents folder using ActiveSync.

Remote Desktop (Auto). A shortcut to Remote Desktop Mobile with Connect activated..

Remote Desktop (page 5-67). Display remote desktop. Setup for computer, user name, password and domain required. Use Options to setup connected options for the remote desktop.

Settings Panels (page 5-14). Access to system level setup programs. Connections Panels (page 5-50), Personal Panels (page 5-23), and System Panels (page 5-29) among others.

Task Manager (page 5-49). View and cancel running tasks.

Tasks (page 5-59). Task list application. Can be synchronized with PC Outlook task list using ActiveSync.

Text. Requires an email application. Can be synchronized with PC Outlook email using ActiveSync or it can synchronize with an Exchange server.

Today (page 5-22). Configure the appearance and the items to display on the Today screen.

Windows Live (page 5-59). Sign in to Microsoft Windows Live online service. Internet access required.

Windows Media (page 5-60). Audio visual management program. Not supported on the MX7 Tecton.

Office Mobile

Excel Mobile (page 5-64). Spreadsheets can be edited, data can be sorted, formatting and changes are preserved.

PowerPoint Mobile (page 5-65). Open, view and edit slides in landscape or portrait format. Zoom and GoTo features enabled.

Word Mobile (page 5-65). Open, view, edit documents. Formats are saved. Spelling checker, cut and paste are available, undo and redo commands.

OneNote Mobile (page 5-66).

Settings

Clock & Alarms (page 5-14). Set Date, Time, Time Zone, and alarms.

Lock (page 5-16). Set password protection.

Power (page 5-18). Review battery status. Set time limit before device is turned off.

Sounds & Notifications (page 5-20) Enable / disable sounds and vibrations. Set volume parameters and assign sound (wav) files to OS events.

Today (page 5-22). Configure the Today screen.

Connections Panels (page 5-50). Set up various connections between a host and the MX7 Tecton.

Personal Panels (page 5-23). Configure Buttons, Input method and Owner information.

System Panels (page 5-29). Review system information. Set up operating system and equipment parameters.

Personal

About Info (or About LXE) (page 5-23). View software, hardware, versions and network IP. No user intervention required.

Buttons (page 5-24). Set functions of programmable buttons.

Input (page 5-26). Set input options for keypad, touch screen and voice.

Owner Information (page 5-28). Set the mobile device owner details (name, phone, etc.). Enter notes.

System

About (page 5-29). Display OS version information. Set device name.

AppLock (Application Locking) (page 6-1). AppLock Administration utility.

Backlight (page 5-31). Set the display backlight brightness and display/keypad backlight timeout. Configure the timeout based on type of power source: battery or external power.

Battery (page 5-33). View voltage and status of the main battery.

Bluetooth Configuration (page 7-1). Set the parameters for Bluetooth device connections. .

Certificates (page 5-34). Manage digital certificates used for secure communication.

Data Collection Wedge (page 8-1) utility for data collected from bar code scans. Set data collection device, notifications, data stripping, prefix/suffix, and vibration (if installed) options. Assign baud rate, parity, stop bits and data bits for COM1 port. Assign collected data manipulation parameters.

Encryption (page 5-35). Enable file encryption on removable storage cards.

External GPS (page 5-36). Configure serial GPS access.

License Manager (page 5-37). View license information for installed licensed applications.

Managed Programs (page 5-37). View install history for .NET programs.

Memory (page 5-38). Display current state of virtual memory.

Mixer (page 5-39). Adjust the input and output parameters – volume, side-tone, and record gain, for headphone, software and microphone.

MX7 Tecton Options (page 5-40). Set various device specific configuration options.

Peripherals (page 5-42). Enable or disable touch screen heater and scanner window heater, if installed. Set the heater trip point in degrees C.

Regional Settings (page 5-43). Set appearance of numbers, currency, time and date based on country region and language settings.

Registry (page 5-45). Load User Defaults, Save User Defaults, Load Factory Defaults, and Warmboot.

Remove Programs (page 5-46). Remove user installed programs.

Screen (page 5-46). Calibrate touch screen, adjust text options.

Task Manager (page 5-49). Display running tasks. Cancel running tasks.

Wi-Fi (page 5-49). Set the parameters for a Summit client.

Connections

Beam (page 5-50). Enable receiving InfraRed and Bluetooth beams. (Not supported on the MX7 Tecton.)

Connections (page 5-51). Configure connections to servers.

Domain Enroll (page 5-52). Enroll in Active Directory domain.

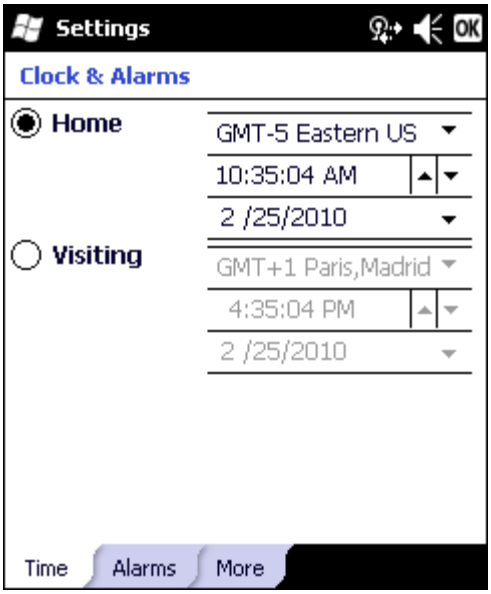
Network Cards (page 5-53). Set the parameters for a wireless network using the utility included in Windows Mobile.

USB to PC (page 5-54). Set up an ActiveSync connection between a host PC and the MX7 Tecton.

Settings Panels

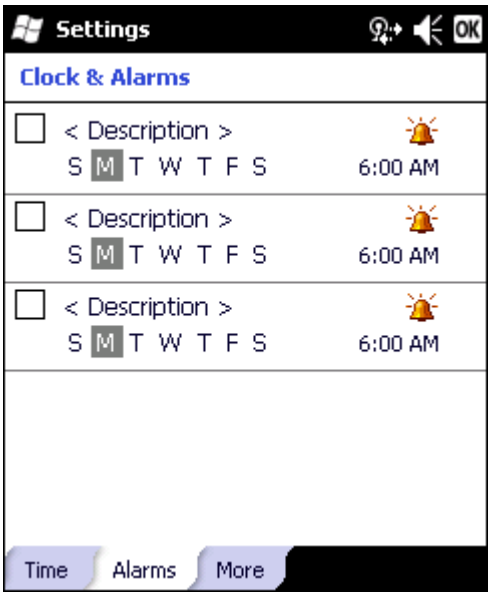
Clock & Alarms

Time



Adjust the settings and tap ok to save the changes. Select Yes on the popup box and the changes take effect immediately. The Time can be set for both a Home and a Visiting location.

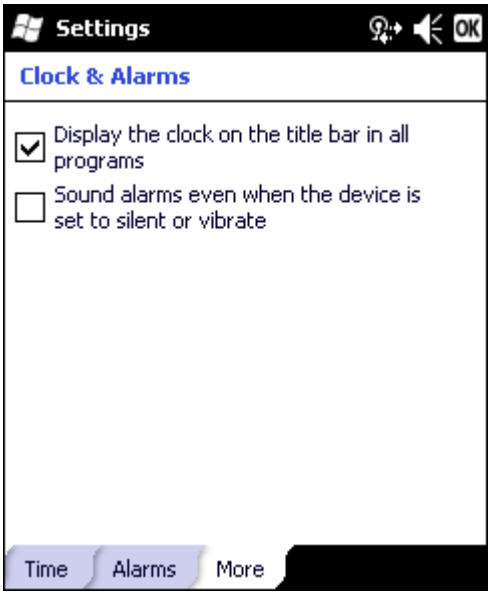
Alarms



To set an alarm:

1. Tap the check box to enable the alarm.
2. Tap **< Description >** and enter a description. The description is limited to 63 characters.
3. Tap the day (or days) to play the alarm.
4. Tap the time to set the time to play the alarm. Set the time and tap ok to return to the Alarms panel.
5. Tap the Bell icon to set the notification. Notifications may include sound, light flash (the Alpha LED flashes) and vibration. Set the desired options and tap ok to return to the Alarms panel.
6. Tap ok when finished to dismiss the Alarms panel.

More



Lock

Password

Set the lock / unlock behavior for the MX7 Tecton.

Setting	Default
Prompt if device unused for	Unchecked
Timer	0 minutes
Password type	Simple PIN
Password	<blank>
Confirm	<blank>
Password hint	<blank>

Prompt if phone unused for

Tap the check box and set the inactivity timeout before the MX7 Tecton locks.

Password type

When selecting a **Password type** the MX7 Tecton displays a numeric keypad or the input panel depending on the type of password selected.

Select the Password type, Simple PIN (numeric) or strong alphanumeric. Enter the desired password and confirm. Note that Windows Mobile places restrictions on what it considers a valid password. If the chosen password is not strong enough, a warning is displayed and a new password should be entered and confirmed.

Note: After a password has been entered, the password must be used to access the Lock panels again.

Hint

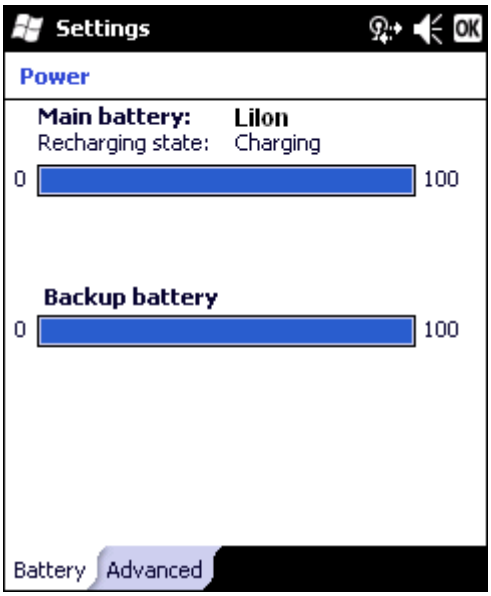
If the password entry isn't successful after a predefined number of attempts, the password hint is displayed.

Power

Reports the current battery state and allows the user to set suspend timeouts.

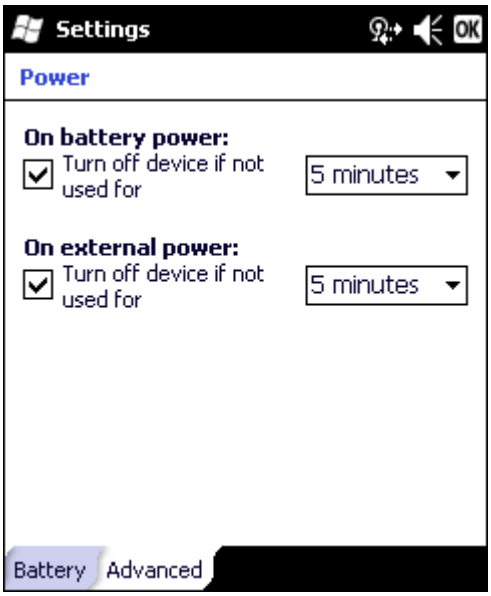
Setting	Default
On battery power:	
Turn off device if not used for	Enabled
Timer setting	5 minutes
On external power:	
Turn off device if not used for	Enabled
Timer setting	5 minutes

Battery



Battery power is displayed for both the main and internal Super-cap batteries (backup battery).

Advanced



Select the inactivity timeout period before the MX7 Tecton goes into Suspend mode. The settings on this panel are for the suspend timers only.

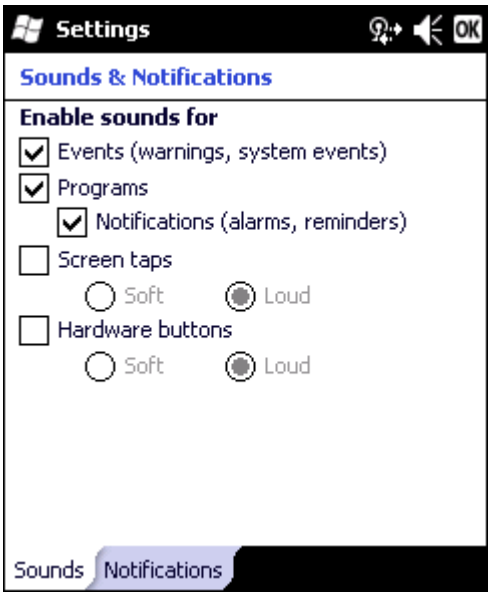
Backlight timers are set using the Backlight (page 5-31) settings panel.

Sounds & Notifications

Set volume parameters and assign sound WAV files to Windows Mobile events. Options that cannot be edited by the user are dimmed.

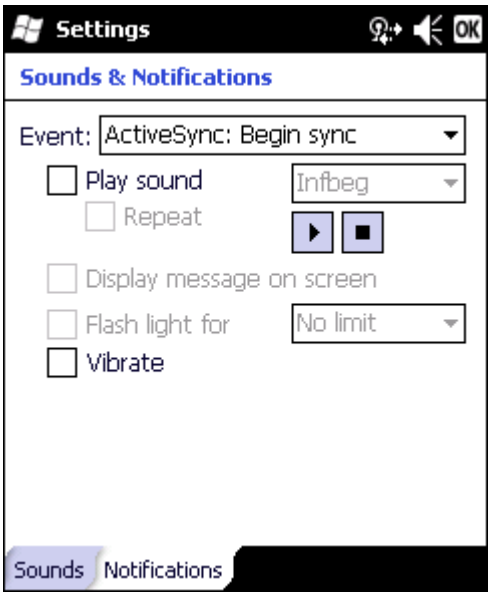
Sounds

Setting	Default
Events	Enabled
Programs	Enabled
Notifications	Enabled
Screen taps	Disabled
Hardware buttons	Disabled



Follow the instructions on the screen and tap OK to save the changes. Changes take effect immediately.

Notifications



The Event box lists several events that can have an associated notification. The notification, depending on the event selected, may consist of playing a sound, displaying a screen message, flashing a light or triggering the vibration motor.

When the flash light option is selected, the MX7 Tecton flashes the Alpha LED.

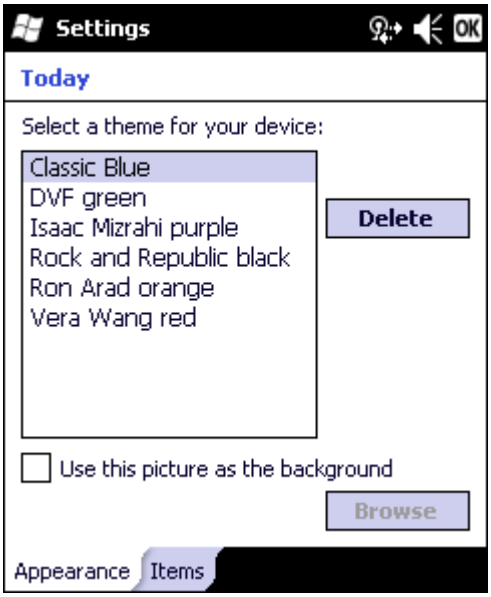
When finished, tap OK to save the changes.

Today

Configure the appearance and the items to display on the Today screen.

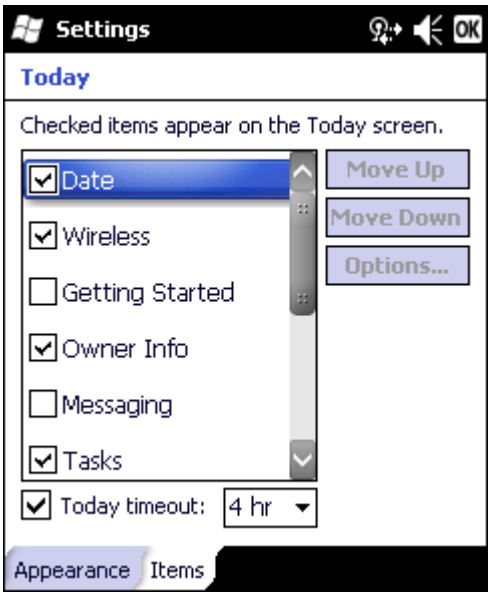
Appearance

Use the Appearance panel to assign a theme for the device. The default theme is Windows Mobile Classic Blue. Any user installed themes are included in the list.



Items

Use the Items panel to select the items to be shown on the Start panel. Calendar must be selected as well as Date if the date is the only item to be shown on the Start menu.



The **Today timeout** timer refers to the “return to Today screen” function. When the device is placed in Suspend, and the timer expires, a return from Suspend displays the Today screen, not the application in focus when the MX7 Tecton was placed in Suspend. The application in focus, which is running in the background, will need to be selected again.

Use **Options** to set display parameters for highlighted items in the Checked Items list.

Personal Panels

About Info (or About LXE)

The data cannot be edited by the MX7 Tecton user on these panels.

Tab	Contents
Software	GUID, Windows CE Version, OAL Version, Bootloader Version, Compile Version, Programmable Component Version(s) and Language. Language indicates localized version.
Hardware	CPU Type, Codec Type, Display, Flash memory, and DRAM memory
Versions	Revision level of software modules and .NET Compact Framework Version. Utilities, Drivers, Image, CE API, and Internet Explorer.
Network IP	Current IP address, MAC address, and gateway address for all network ports (802.11 radio, ActiveSync).

Software

The Software tab may display the current language. All languages are built into the OS image; English, French, German, Simplified Chinese, Traditional Chinese, Japanese, Korean, Spanish, Thai. .

Hardware

The Hardware tab displays hardware information such as CPU, keyboard type, display and memory.

Version

The Versions tab displays the versions of many of the software programs installed. Not all installed software installed on the MX7 Tecton is included in this list and the list varies depending on the applications loaded on the MX7 Tecton. The Image line displays the revision of the system software installed. Refer to the last three digits to determine the revision level.

Version window information is retrieved from the registry.

Modify the Registry using the Registry Editor. Use caution when editing the Registry and make a backup copy of the registry before changes are made.

The registry settings for the Version tab are under HKEY_LOCAL_MACHINE \ Software \ LXE \ Version in the registry.

To add a user application to the Version panel, create a new string value under the HKLM\Software\LXE\Version key. The string name should be the Application name to appear in the Version window. The data for the value should be the version number to appear in the Version window .

Version strings can be equal to or less than 254 characters. Because the strings are displayed in a text box, any number can be accommodated, up to the 64K byte text box limitation.

Network

The Network IP tab displays the MAC address of the network adapter(s) plus IP address and gateway for connected adapters.

Buttons

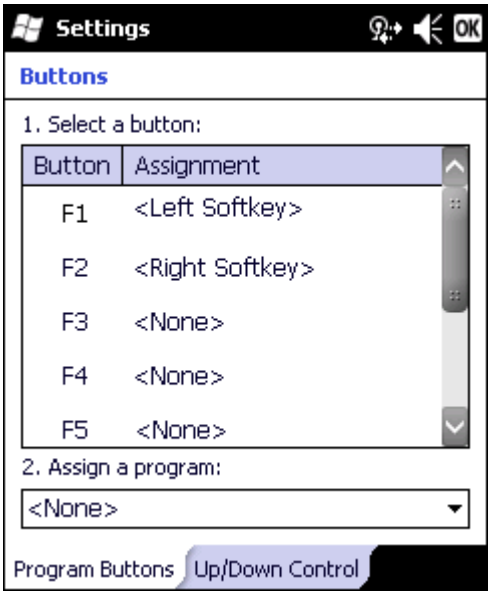
Program Buttons

Program buttons can be used to assign functions to certain keys such as F1 through F5 and the diamond keys. Buttons can only be assigned to programs that have an icon in the Start menu or the Settings folder (including sub-folders). A program that is not in the above mentioned locations does not show up in the list here.

Note: The button links to the shortcut to the program, not the executable file.

Note: The System Administrator uses the Buttons setting panels to assign a Status User key and a Status Admin key on the Status Popup panel, see Status Popup (page 5-41).

Setting	Default
32-Key Keypad	
F1	Left Softkey
F2	Right Softkey
F3, F4, F5, D1, D2, D3	<None>
55-Key Keypad	
F1	Left Softkey
F2	Right Softkey
F3, F4, F5, D1	<None>

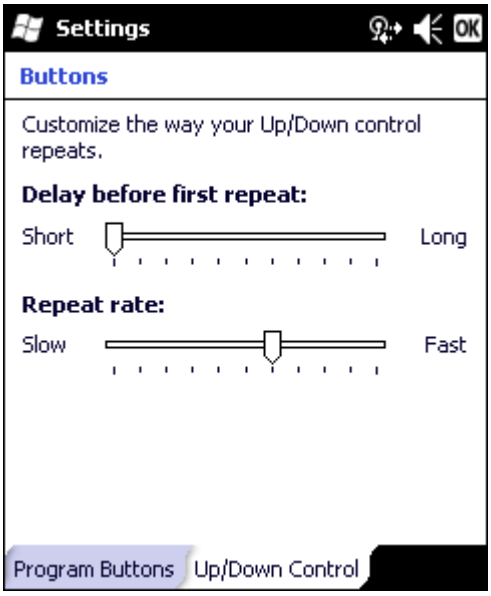


To assign a button:

1. Tap to highlight the desired button.
2. Select the program or shortcut from the Assign a program drop down box.
3. Tap ok.

Up/Down Control

Customize the delay before repeating and the repeat rate for the up/down controls.

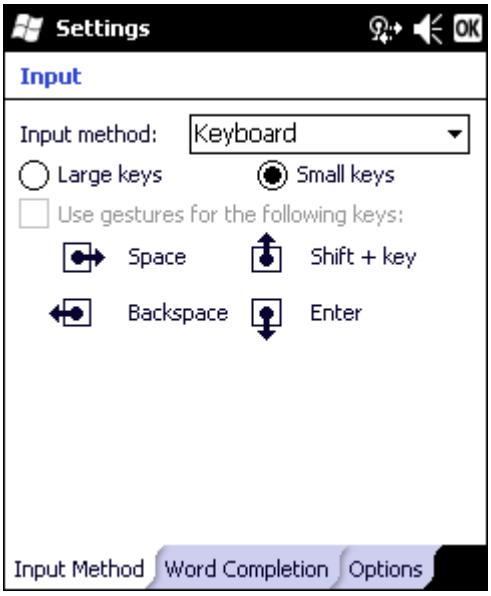


Input

Setting	Default
Input Method	Keyboard
Small keys	Enabled
Word Completion	
Suggest words when entering text	Enabled
Suggest after entering	A space
Suggest number word(s)	4
Add a space after word	Enabled
Enable auto correct	Enabled
Options	
Voice recording format	8000 Hz, 8 Bit, Mono
Default zoom level for writing	200%
Default zoom level for typing	100%
Capitalize first letter of sentence	Enabled
Scroll upon reaching the last line	Enabled

Input Method

Select the preferred method of input.

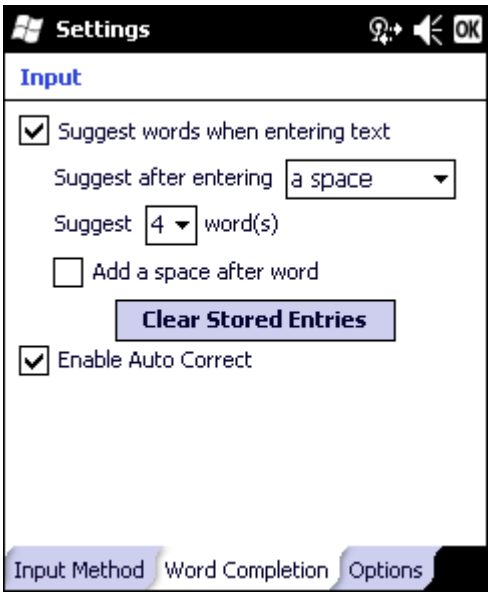


The default method of input is the keyboard or input panel. When the cursor is located in a field allowing text input, the input panel may automatically be displayed. If not automatically displayed, the input panel can be accessed by tapping on the keyboard icon at the bottom center of the screen.

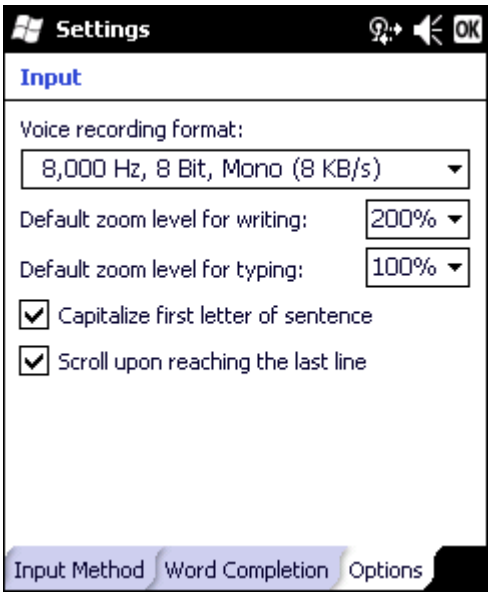
If a different input method is active, the icon for that input method is displayed instead of the keyboard icon.

Tap ok to save any changes.

Word Completion



Options



Owner Information

Set the MX7 Tecton owner details.

Identification	
Name, Company, Address, Telephone, E-mail	Blank
Notes	
Notes	Blank

Enter the information and tap ok to save the changes. The changes take effect immediately.

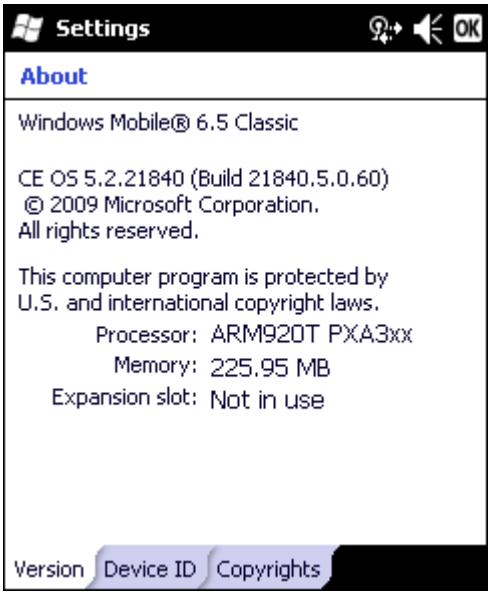
*Note: Owner Identification name listed in **Start > Settings > Personal > Owner > Information** is not used during Bluetooth operation.*

System Panels

About

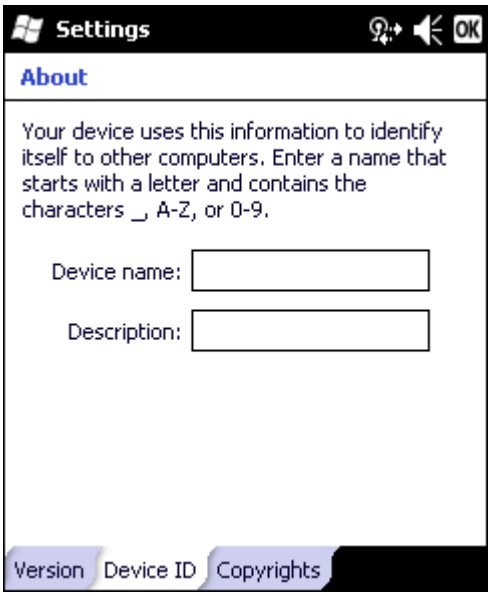
The About panels show OS versions, allow device name and description input and display copyright information.

Version



This screen displays information on the installed operating system and the hardware. Note that Windows Mobile is based on a Windows CE engine. The underlying version of Windows CE is displayed here.

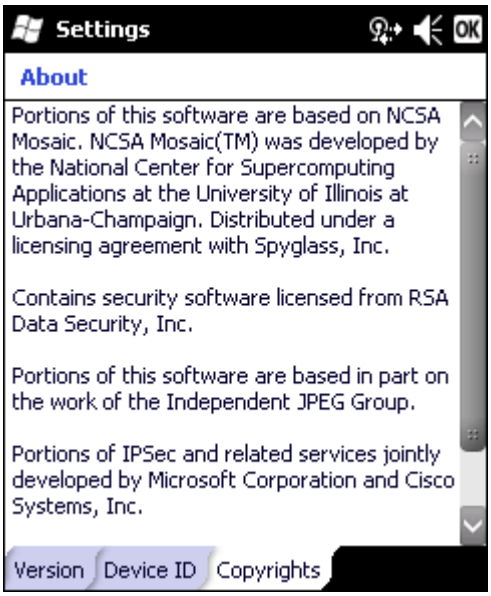
Device ID



The device name and description can be changed by the user. Enter the name and description using either the keypad or the Input Panel and tap ok to save the changes. The changes take effect immediately.

*Note: The Device name listed in **Start > Settings > System > About > Device ID** is not used during Bluetooth operation.*

Copyrights



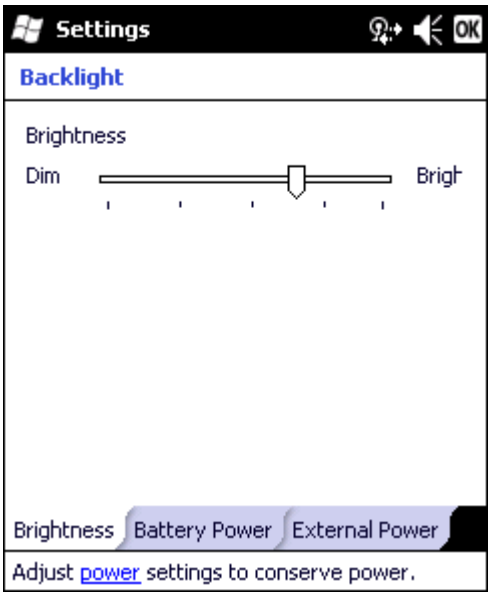
This screen is presented for information only. The Copyrights information cannot be changed by the user.

Backlight

Set the power management timers for the display and keypad backlights. Set the display brightness for battery and external power.

Setting	Default
Brightness	60%
Battery Power	
Turn off backlight if device not used for	30 seconds
Turn on backlight when a button is pressed or the screen is tapped	Enabled
External Power	
Turn off backlight if device not used for	1 minute
Turn on backlight when a button is pressed or the screen is tapped	Enabled

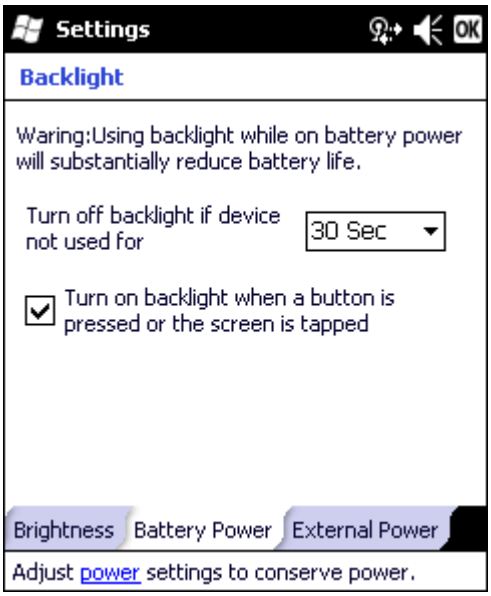
Brightness



Slide the marker left and right to select the desired keypad and display brightness level. Adjust the settings and tap OK to save the changes. The changes take effect immediately

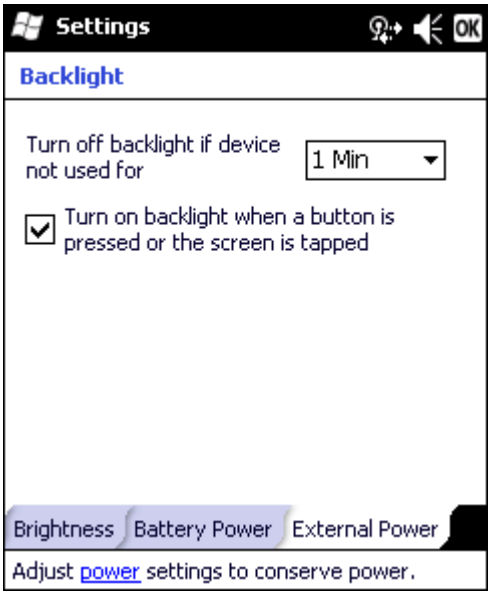
When the backlight timer expires, the display backlight and the display are Off, as is the keypad backlight. This is the System Idle state, there is no separate User Idle state.

Battery Power



When the MX7 Tecton is on battery power and the backlight timer expires, the display and the backlights for the display and keypad are turned off. Adjust the settings and tap OK to save the changes. The changes take effect immediately.

External Power



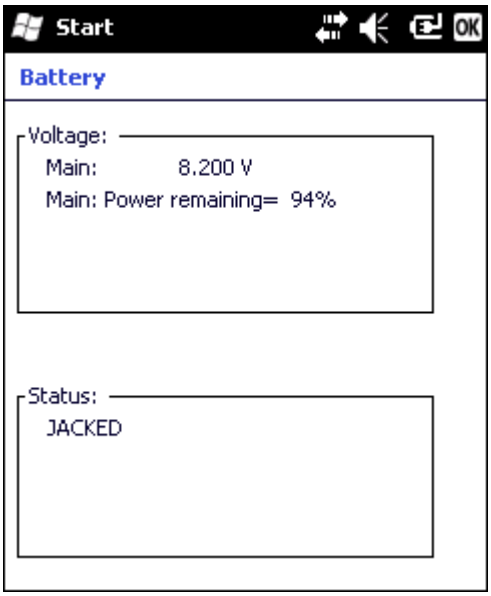
When the MX7 Tecton is on external power and the backlight timer expires, the display and the backlights for the display and keypad are turned off. Adjust the settings and tap OK to save the changes. The changes take effect immediately.

Battery

This panel is used to view the status and percentage of power remaining in the MX7 Tecton main battery.

Jacked is shown in the Status box when the Main battery is receiving external power.

The main battery is charged/recharged when the MX7 Tecton is docked in a powered cradle or directly cabled to an external power source.



The internal battery draws power from the Main battery to maintain a charge. The Super-cap battery voltage and percentage of power fluctuate continuously.

When there is no Main battery in the unit, the internal battery begins to discharge as it maintains RAM and other vital settings. After a Main battery is installed, the internal battery begins to draw power from the Main battery again and is fully recharged in five minutes or less.

Note: Frequent connection to an external power source, if feasible, is recommended to maintain main battery charge status as the Super-cap battery cannot be recharged by a dead or missing main battery.

Certificates

Manage digital certificates used for secure communication.

View – displays details of the certificate. Personal certificates may be extended from the view screen.

Delete – removes the certificate from the device. Delete is not available if the certificate was installed by a device administrator.

Certificates are divided into three types: Personal, Intermediate and Root.

See Certificates (page 11-36) chapter for detailed instruction on generating certificates.

Personal

This panel lists any installed Personal certificates. Personal certificates are used to identify the user of the device.

To install a User certificate:

1. Copy the .pfx or .p12 file to a folder on the MX7 Tecton.
2. Use File Explorer to browse to the location of the file and open the file by tapping the file name.
3. Type in the password to unlock the certificate and tap Done.
4. The new certificate is copied to the Personal certificate store on the MX7 Tecton.

Intermediate

This panel lists any installed Intermediate certificates. Intermediate certificates are used to help authenticate certificates received from other hosts.

To install an Intermediate certificate:

1. Copy a DER-encoded .cer file, a base64-encoded .cer file or a .pfx file to a folder on the MX7 Tecton.
2. Use File Explorer to browse to the location of the file and open the file by tapping the file name.
3. The new certificate is copied to Intermediate certificate store on the MX7 Tecton.

Root

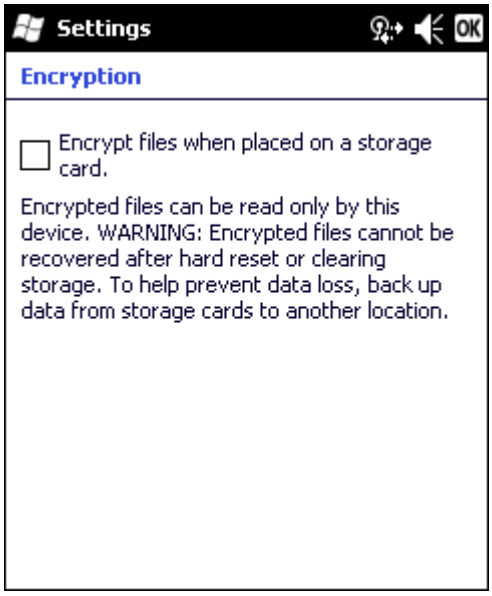
This panel lists any installed Root certificates. Root certificates are used to authenticate certificates received from other hosts.

To install a Root certificate:

1. Copy a DER-encoded .cer file, a base64-encoded .cer file or a .pfx file to a folder on the MX7 Tecton.
2. Use File Explorer to browse to the location of the file and open the file by tapping the file name.
3. The new certificate is copied to Root certificate store on the MX7 Tecton.

Encryption

This panel enables or disables encryption of data files on removable storage cards. The default is Disabled. Tap the check box to encrypt files when placed on a storage card.

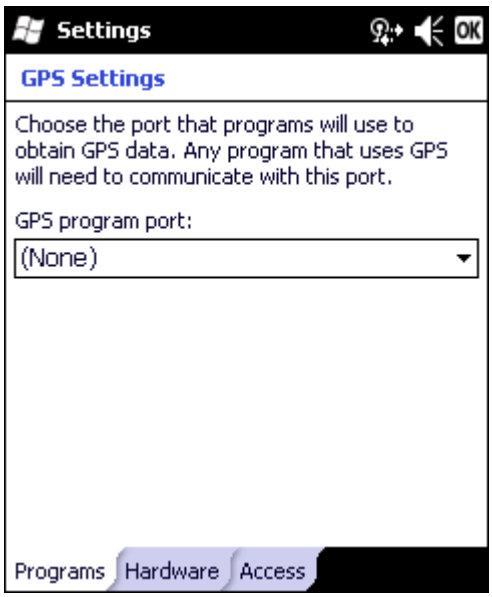


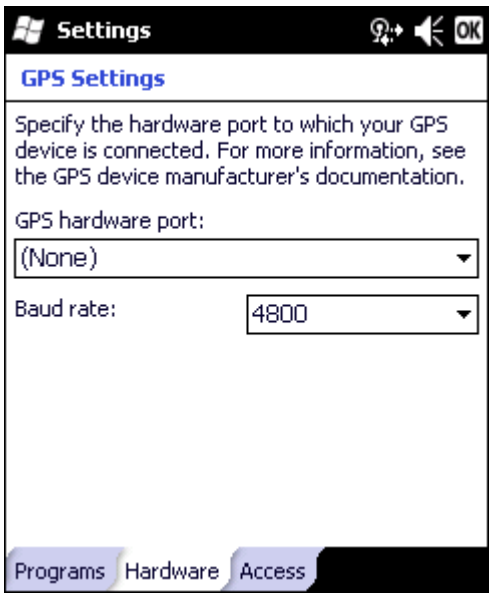
External GPS

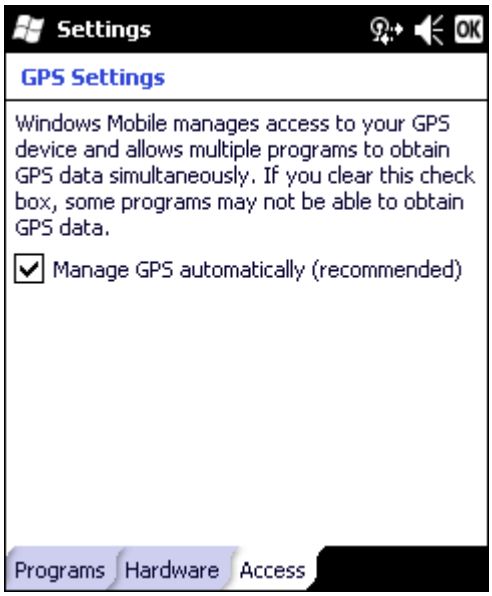
Setting	Default
GPS Program Port	None
GPS Hardware Port	None
Baud Rate	4800
Access	Automatic

This panel configures serial GPS access over hardware serial ports using the Microsoft GPS manager. The port used, baud rate and port sharing must be specified.

In order to use the configuration items on these panels, GPS applications must use the Microsoft GPS API interface rather than reading the serial port directly. If the GPS application reads the serial port directly, these settings are not necessary.



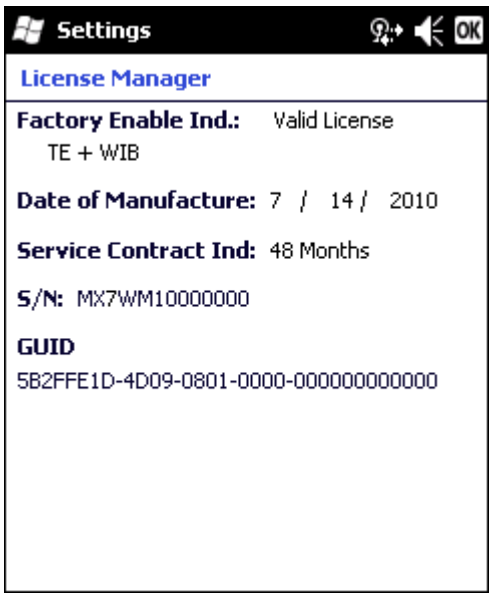




License Manager

Use this option to view software license registration details, and service contract length for purchased software installed on the MX7 Tecton. Note the following image is a sample screen.

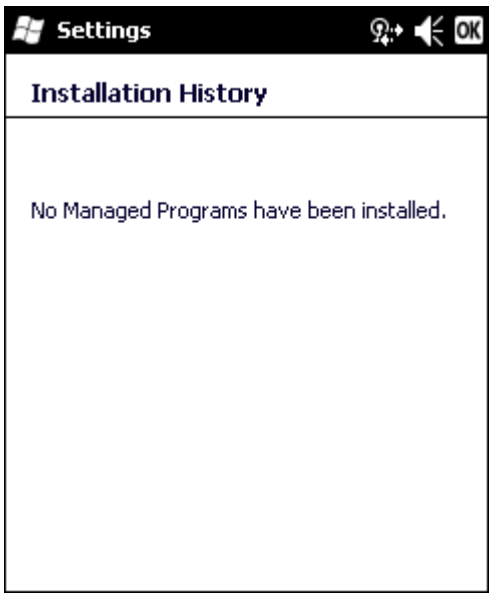
Your License Manager panel may show more tabs, e.g., RFTerm, depending on the number of software applications running on the MX7 Tecton that require a license.



Software and driver version information is located in About (page 5-29). Copyright information is located in the Copyrights tab of the About control panel.

Managed Programs

This panel displays the install history for .NET managed programs. The list is read only.

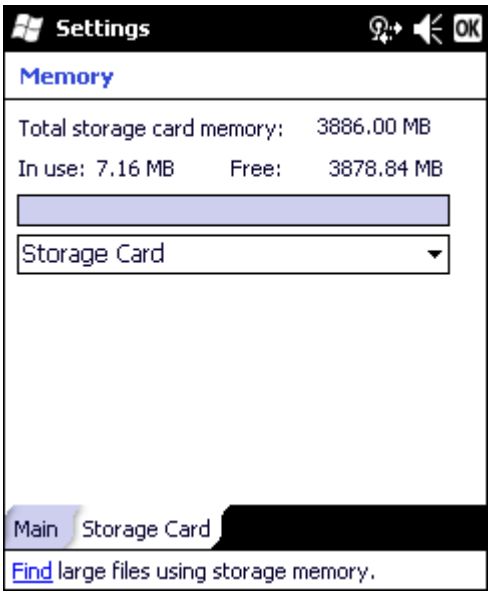


See Remove Programs (page 5-46).

Memory

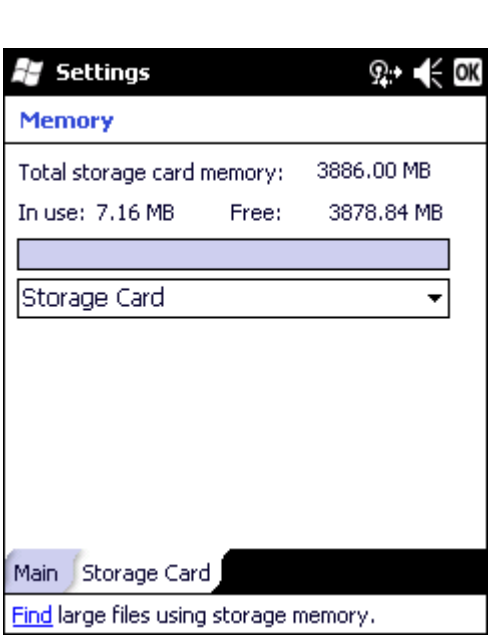
These panels report the current state of virtual memory.

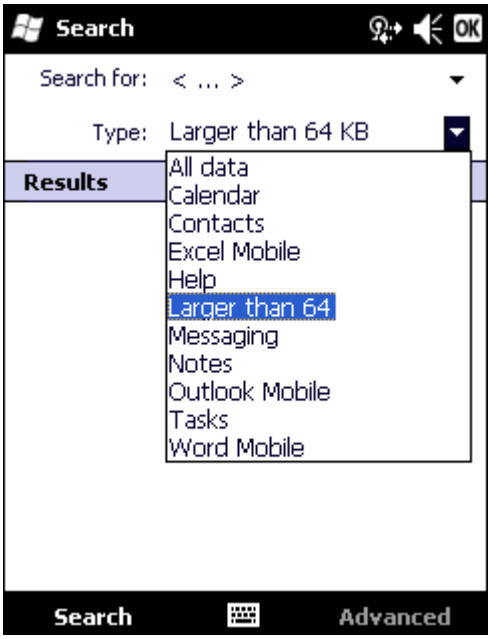
Main



The split between Storage memory and Program memory is not adjustable.

Storage Card





The pop-up list shows all mounted storage, both fixed and removable.

The Find prompt at the bottom of the screen launches the Search utility.

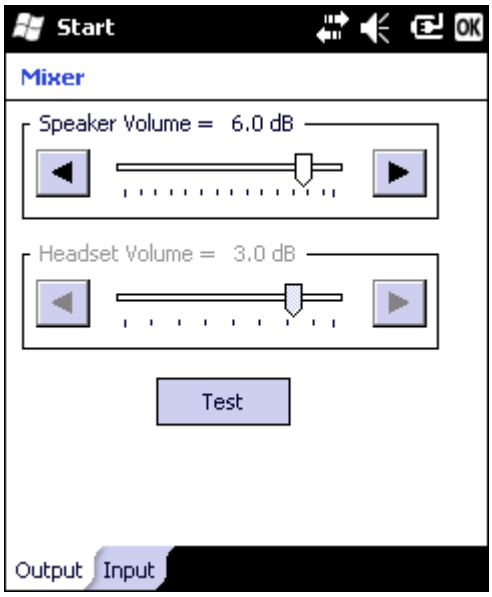
Mixer

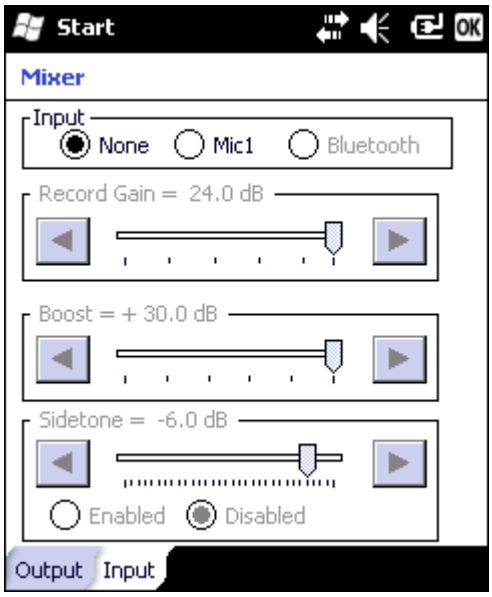
The MX7 Tecton has a speaker located above the scan button. It is active when a headset is not connected to the device.

Use the settings on these panels to adjust the volume, record gain and sidetone for microphone input, speaker and speaker output.

Headsets can be enabled, disabled and selected using these panels.

Setting	Default
Output	
Speaker Volume	6.0 dB
Headset Volume	3.0 dB
Input	
Input	Mic1
Record Gain	24.0 dB
Boost	+ 30.0 dB
Sidetone	6.0 dB / Disabled





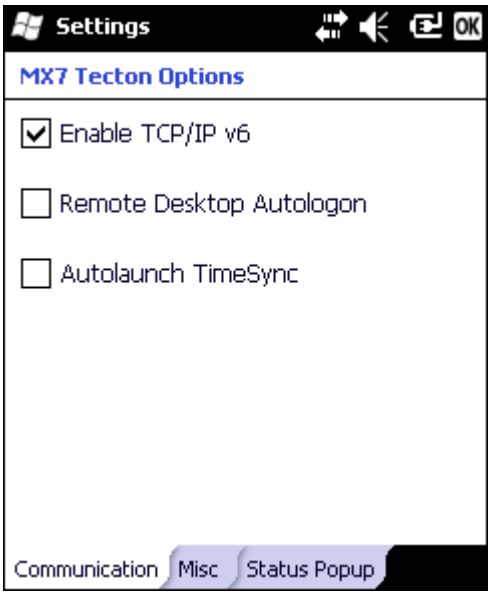
Tap and hold the sliders and move them either left or right, or tap the left and right arrows, to adjust decibel levels.

Tap the Test button on the Output panel to hear a changed setting.

MX7 Tecton Options

Set MX7 Tecton specific device options. Options that cannot be edited by the user are dimmed.

Communication

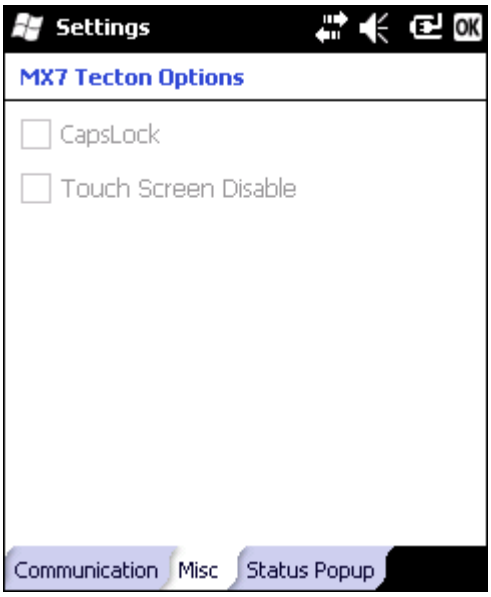


By default, TCP/IP version 6 is enabled on the MX7 Tecton. Tap to uncheck this check box to disable TCP/IP version 6.

By default, Remote Desktop Autologin is disabled. Tap this check box to enable Remote Desktop Autologin.

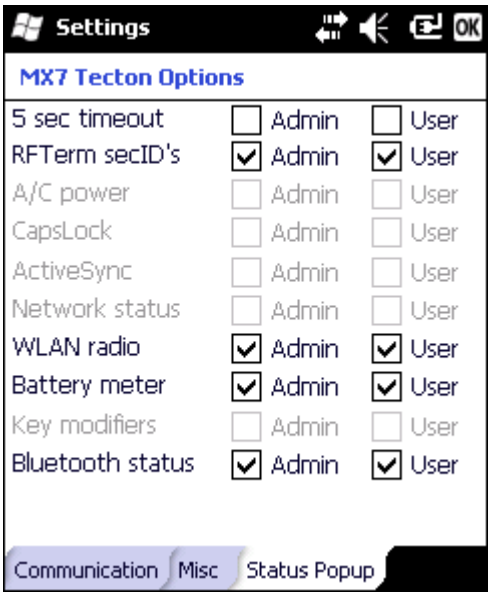
Autolaunch TimeSync enables time synchronization when the MX7 Tecton boots.

Misc



There are no user configurable options on this screen.

Status Popup



When the Status popup window is enabled, and displayed, it is placed on top of the window in focus and hides any data beneath it.

The Status Popup window is closed by pressing the assigned Status User or Status Admin key sequence.

Note: Use a Diamond key for the assigned key sequence to use when opening and closing the popup. If a Function key is used, that Function key is not available to applications that generally use Function keys such as RFTerm.

Using the Buttons settings panel (**Start > Settings > Personal > Buttons > Program Buttons**), the System Administrator must first assign a Status User key for the end-user when they want to toggle the Status Popup Window on or off. Select the desired key and assign that key to StatPopup.

Similarly the System Administrator must also assign a Status Admin key to perform the same function for the Admin popup. Select the desired key and assign that key to Admin StatPop.

Status popup window display options (taskbar icons) are assigned on the Status Popup tab. E.g., WLAN radio, Battery meter, Bluetooth status, RFTerm SecID's (Secondary IDs), etc.

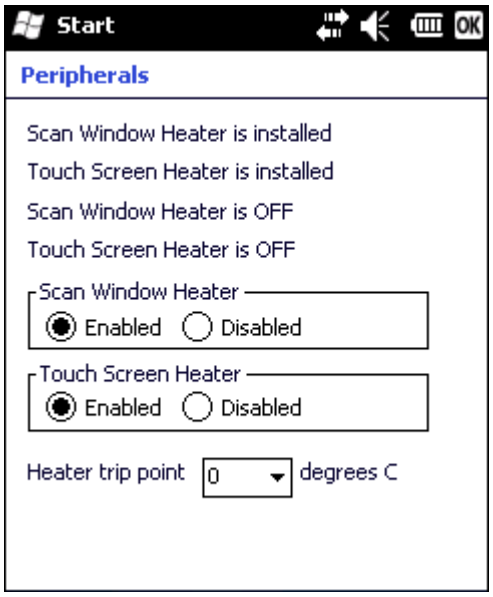
The default is for the User and Admin status popup windows to show all status information. The 5-second timeout to remove the status popup from the display is disabled by default for the User and Admin status popup windows.

Peripherals

This panel is used to enable and disable the touch screen heater and scan window heater.

Setting	Default
Touch screen heater	Enabled
Scan window heater	Enabled
Heater Trip Point	0° C / 32° F

Note: Settings have no effect if the touch screen / scan window heaters are not installed.

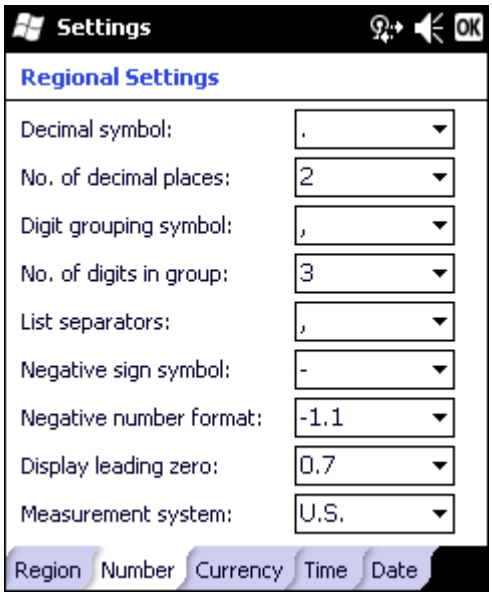


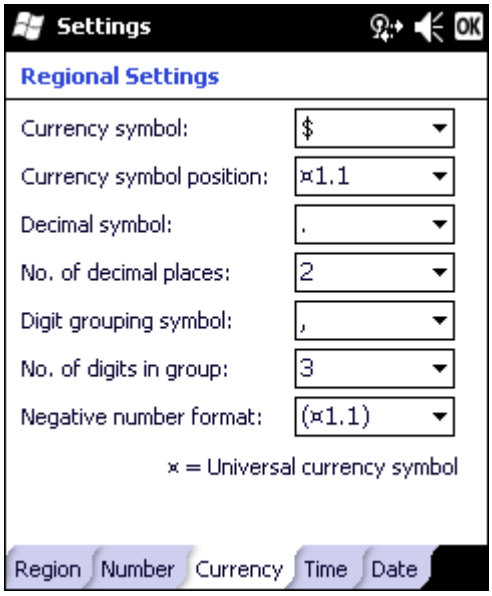
Click the radio button to enable or disable the heaters.

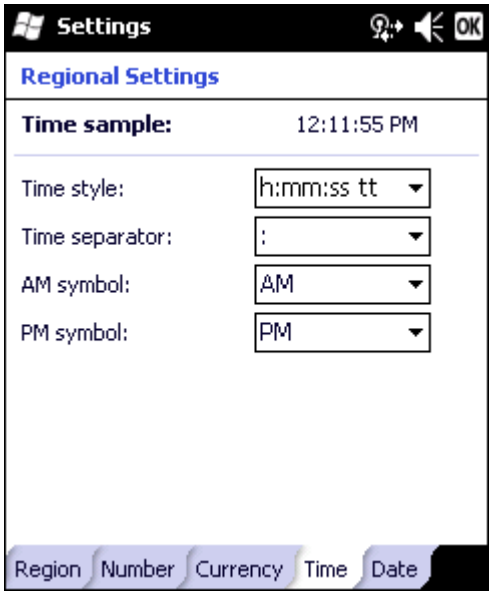
Choose a different trip point from the drop down list and tap OK. The change is in effect after the Peripherals panel is saved.

Regional Settings

Regional Settings has the same general format and function as Regional Settings on a PC.



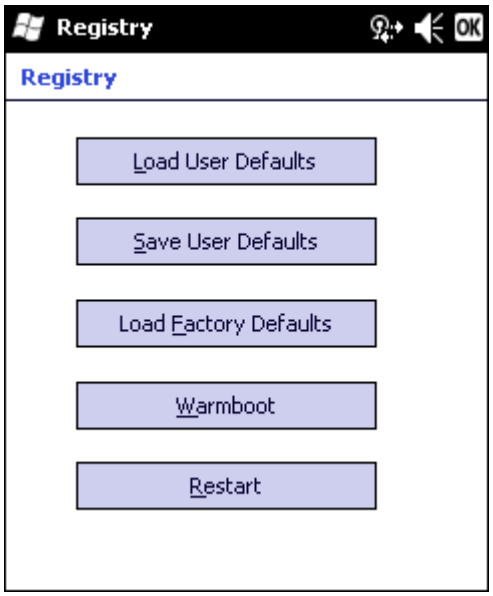





Settings
OK
Regional Settings
Short date: 8/2/11
Long date: Tuesday, August 02, 2011
Short date: M/d/yy
Date separator: /
Long date: dddd, MMMM dd, y
Calendar type: Gregorian Calendar
Region
Number
Currency
Time
Date

Registry

Choose an MX7 Tecton software reload scheme.



Load User Defaults

When clicked, a standard load file dialog is opened, to allow the user to pick a Registry Save (.RSG) file. The applet then copies the specified User registry file to the Active registry. The user is asked to verify a reboot, and then the applet does a warmboot to activate the new registry.

Load User Defaults takes 20 seconds from SD card, or 10 seconds from internal flash.

Save User Defaults

When clicked, a standard Save File dialog is opened, to allow the user to name the Registry Save (.RSG) file. The applet then copies the Active registry to the specified User registry file.

Save User Defaults takes 30 seconds to save to SD card, or 10 seconds to save to internal flash.

Load Factory Defaults

The applet copies the Factory Default registry from the OS to the Active registry (by deleting the current registry). The user is asked to verify a reboot, and then the applet does a restart to activate the factory default registry. If a user password has been set, the applet warns the user that the password will be erased, and asks them to enter it before the reboot is allowed.

Warmboot

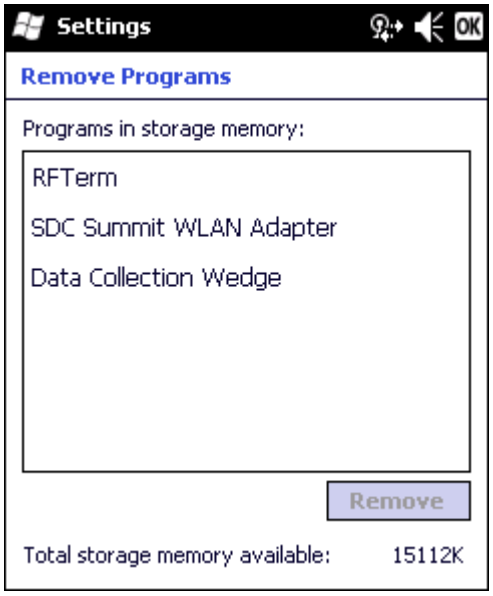
When clicked, the OS does a registry flush (Active registry saved to Flash registry hive), and then a warmboot.

Restart

When clicked, the OS does a registry flush, and then a restart.

Remove Programs

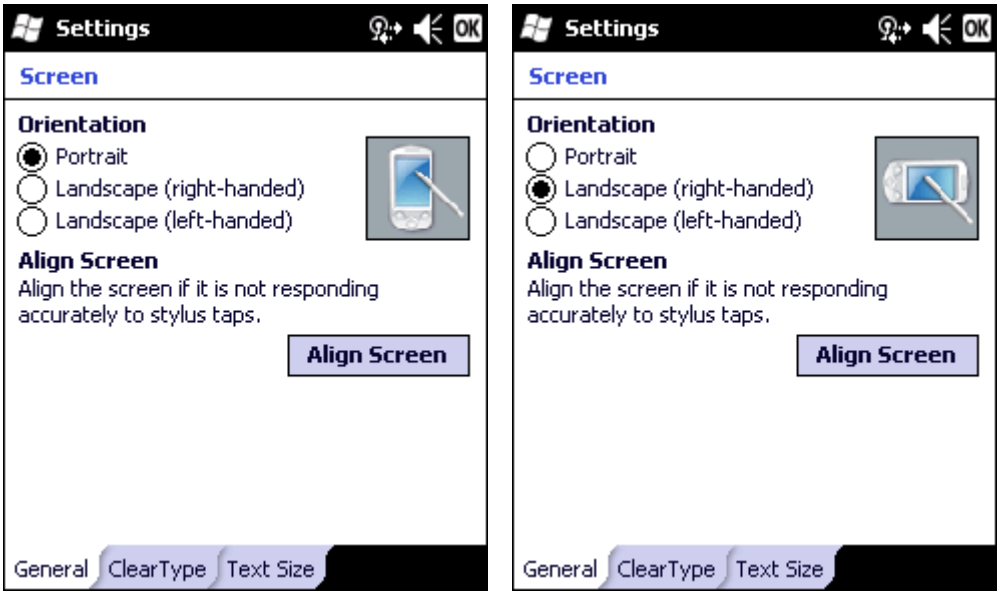
This panel is used to uninstall programs. The Remove Program listing is for all programs installed via ActiveSync or via a CAB file. Programs installed via a package file are not included in this list.



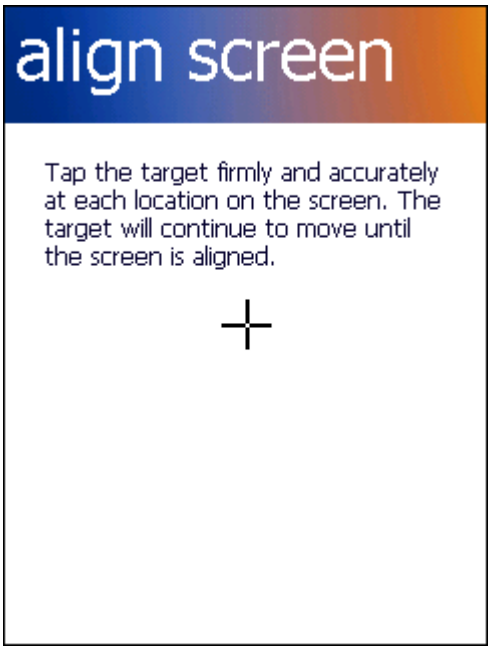
Screen

Use the options on these panels to switch screen orientation, align or calibrate the touch screen and select Clear Type.

General

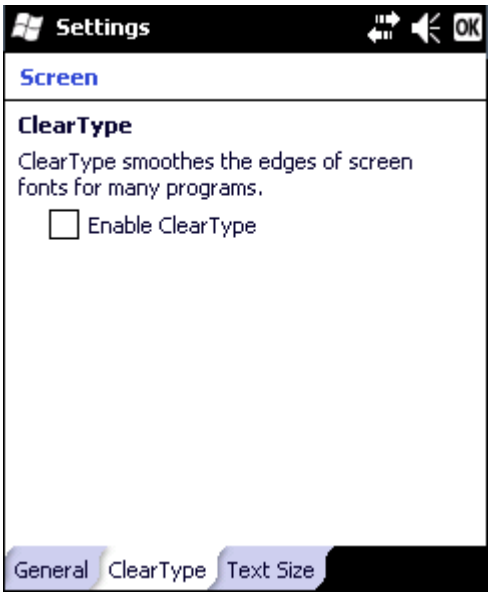


Align Screen

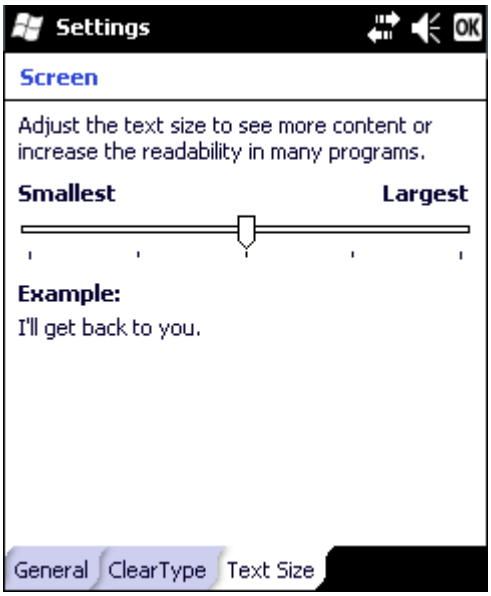


Tap the Align Screen button. The align screen opens and displays a large cross-hair in the middle of the screen. Tap the middle of the cross-hair as it moves around the screen. When the process is complete, the General screen is displayed. Tap ok and the changes are saved. The new alignment is in effect immediately.

Clear Type



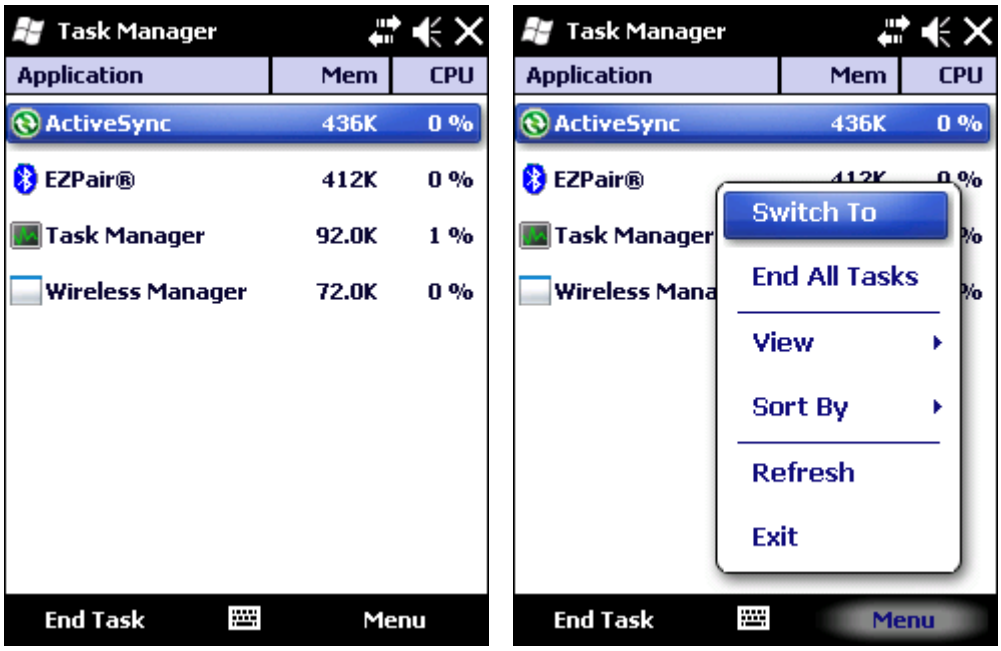
Text Size



Tap the marker and slide it across the bar. As the marker moves, the example text increases or decreases. Tap ok and the change is saved. The new text size is in effect immediately.

Task Manager

This panel displays all running tasks as well as the memory and CPU bandwidth being used by each task.



Tapping on the column headings at the top of the screen sorts the tasks by the contents of that column. Tapping the same heading a second time reverses the sort order of that column.

Highlight an application then tap End Task. More options are available in the Task Manager Menu.

Highlighting then right-clicking on an application displays a popup menu with the following choices:

- Switch To – Switch to the highlighted task. Double-clicking on the task name also performs this function.
- End Task – End the selected task only.
- End All Tasks – End all tasks.

The list is reset by cold boot (or restart).

Note: Any Windows Mobile program that has been run, even if the program has been exited, remains in memory ready to run again. If memory runs out, the programs are released from memory. However, to avoid out of memory operational problems, it is best to manually terminate unwanted tasks using this option.

Wi-Fi

Use this option to set parameters and manage profiles for the wireless client pre-loaded on your MX7 Tecton.

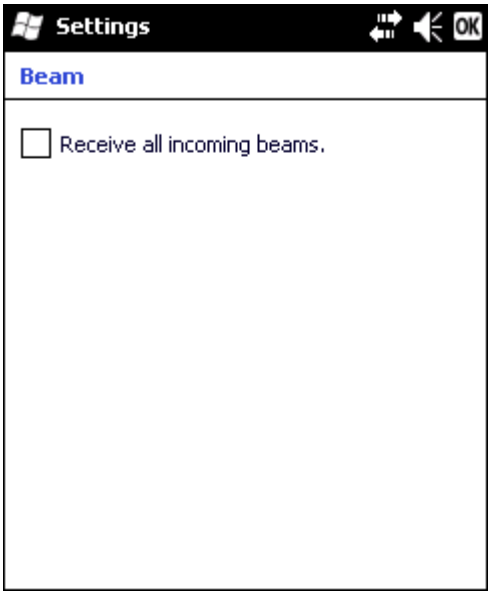
See Summit Client Utility (page 11-1) for more information.

Connections Panels

Beam

Enable or disable receiving OBEX (oBject EXchange is a communications protocol used to exchange information between mobile devices. The devices must support infrared communication.) data beams, either by IrDA (Infrared Data Association, also used as an abbreviation for the Infrared [IR] port on devices.) or Bluetooth.

Note: The MX7 Tecton does not support beaming.

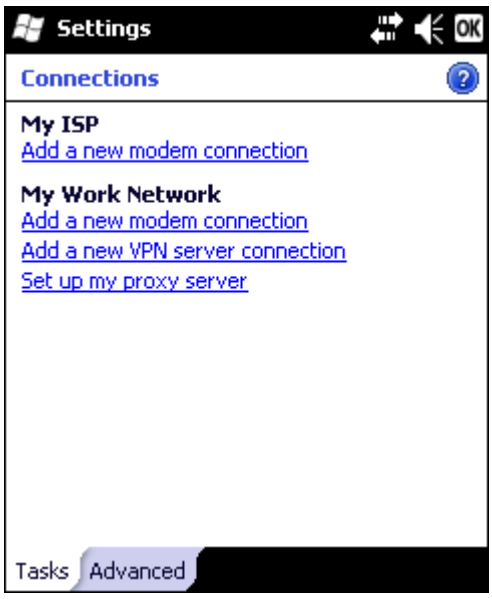


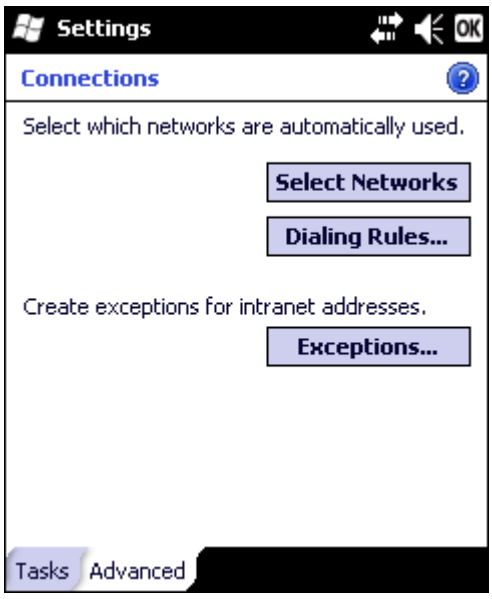
Beam Settings is disabled as the MX7 Tecton does not support beaming.

Connections

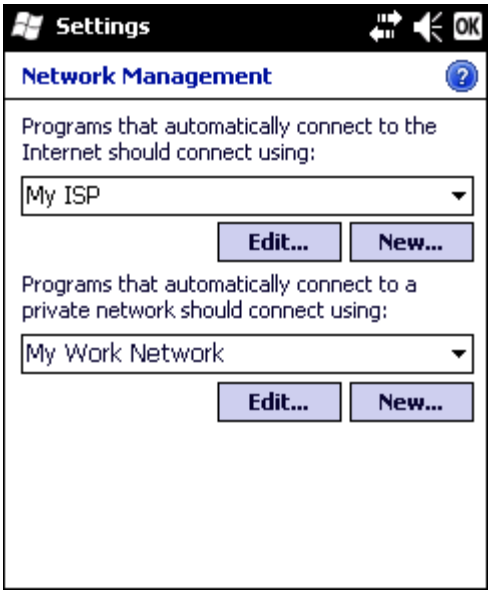
Start > Settings > Connections > Connections

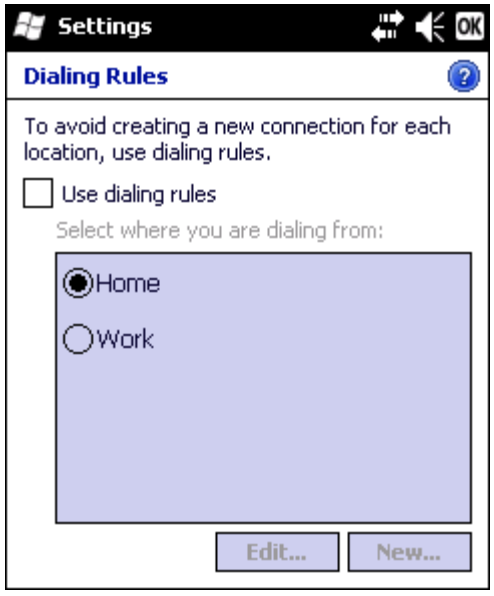
Configure connections to a host PC.

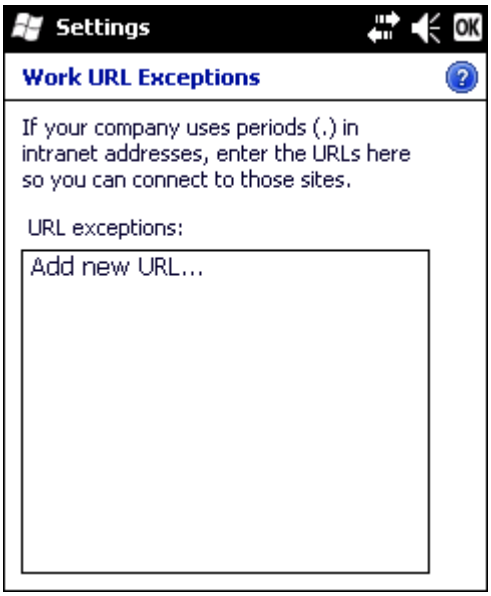




Advanced Options

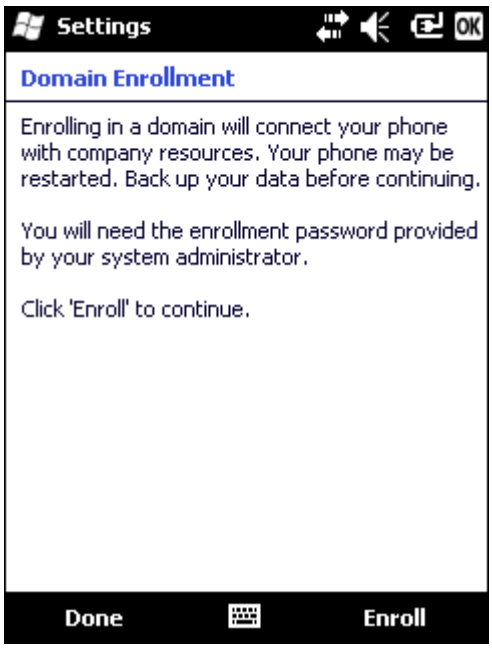






Domain Enroll

Enroll in Active Directory.

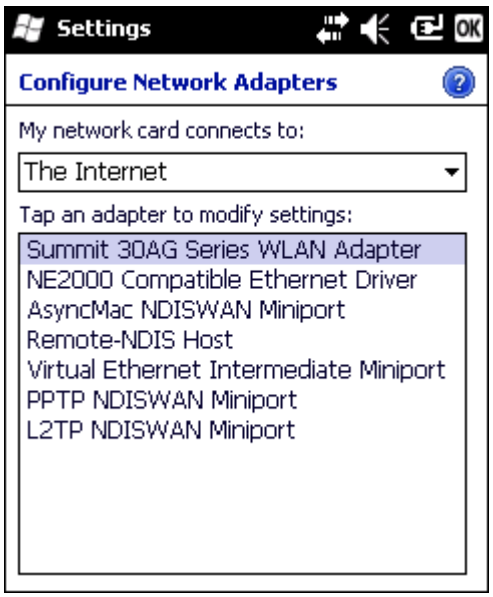


To begin enrollment, tap Enroll in the Status bar. Contact your system administrator for the applicable information to complete the screens.

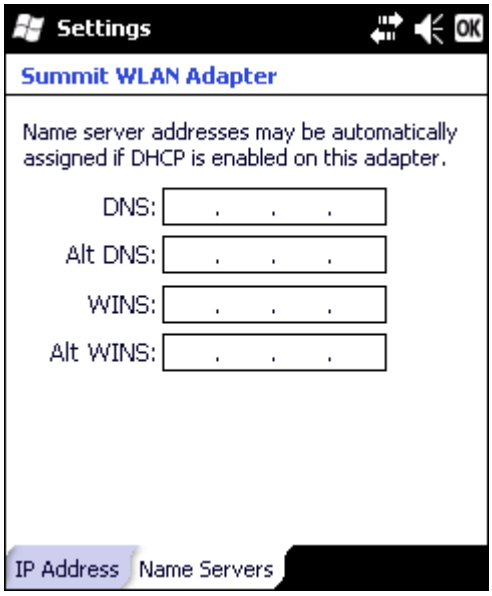
Network Cards

This panel displays a listing of network adapters. The list is based on drivers installed in the registry whether the adapter is actually supported by the hardware or not.

The Network Cards may not always be displayed. If this icon is not displayed, access Network Cards by selecting **Start > Settings > Connections > Wi-Fi > Network Cards** tab.

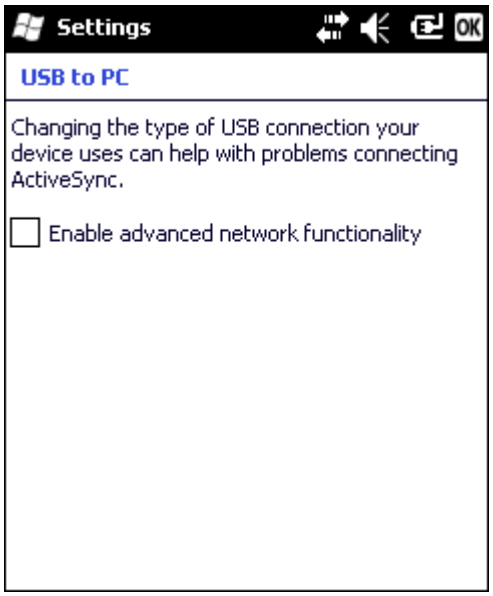


To configure a network card, tap on the adapter name and enter the IP address (or select Use server assigned IP address) and the name server addresses.



USB to PC

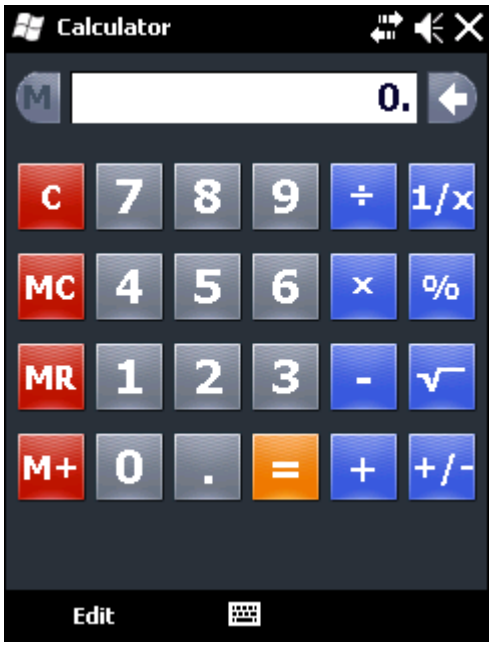
The option is disabled by default. This option can be enabled when connection to a host PC using a USB cable is required.



Standard Microsoft Applications

Note: The intent of this segment is to document standard Microsoft applications loaded on the MX7 Tecton. Documentation only consists of a panel and minimal explanation. These are standard Microsoft small form applications for which help is available using Help on the MX7 Tecton and the Internet.

Calculator



Mathematical calculator application. Use Copy (Ctrl+C) and Paste (Ctrl+V) to move results between applications.

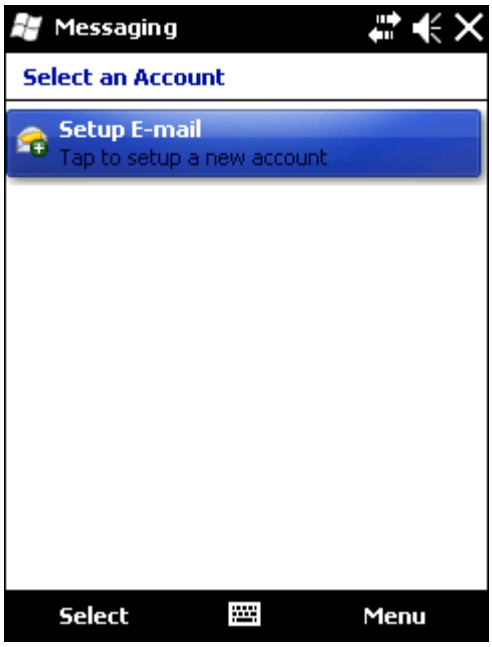
Calendar

Calendar/date book application. Can be synchronized with PC Outlook calendar using ActiveSync.

Contacts

Address book application. Can be synchronized with PC Outlook address book using ActiveSync.

Email

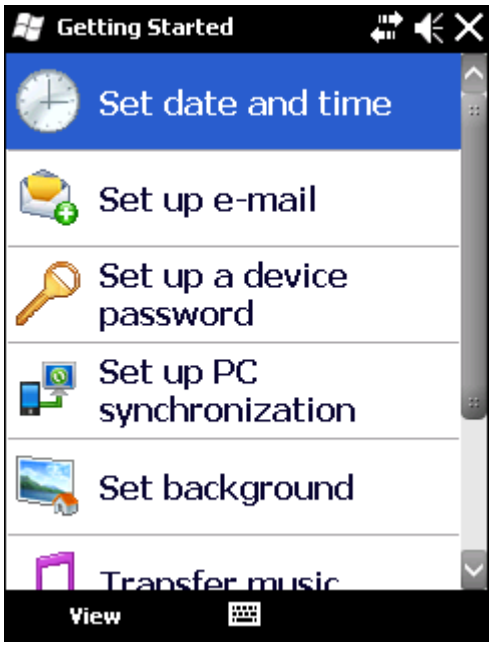


Email application. Can be synchronized with PC Outlook email using ActiveSync or it can synchronize with an Exchange server.

File Explorer

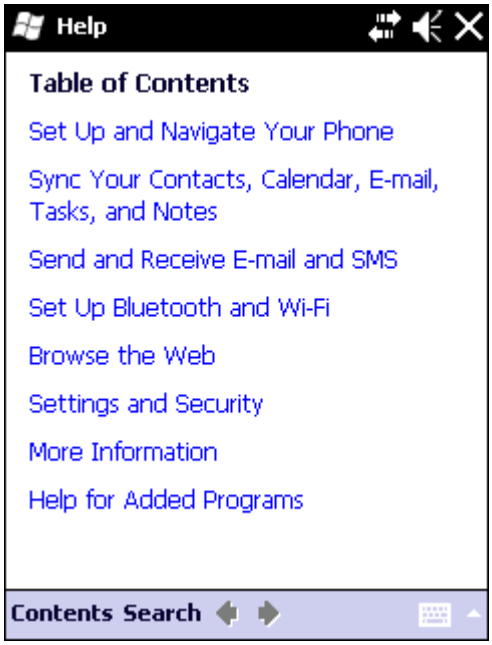
Displays a structured picture of files on the system.

Getting Started



This application provides several wizards to walk a user through device configuration.

Help

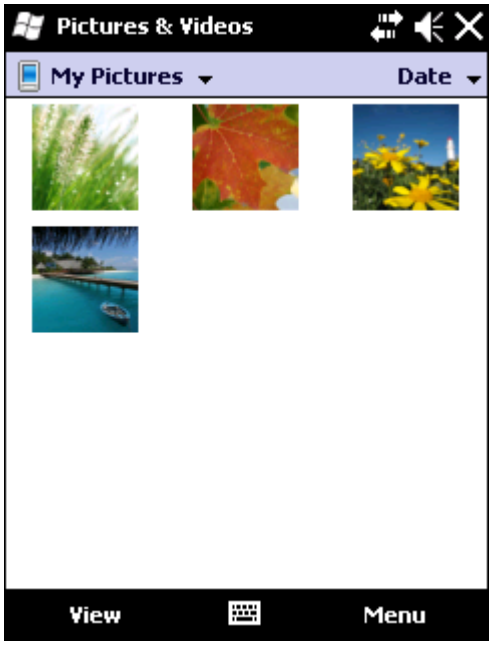


Access Windows Mobile help system on the MX7 Tecton. Options to search using Windows Live Search are available.

Notes

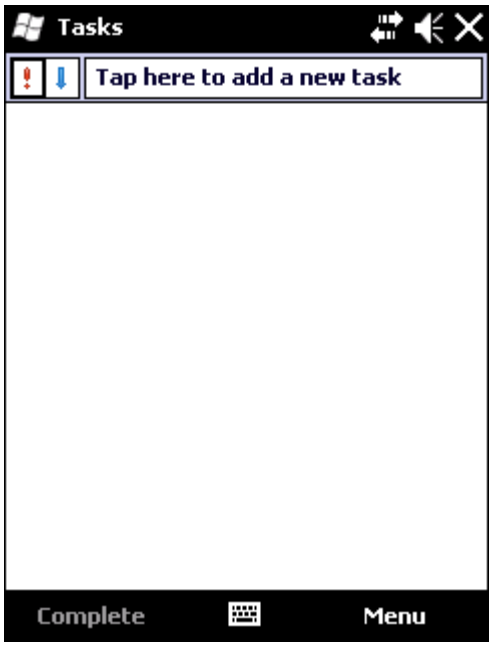
Notes. Notebook application. Select **Menu > View Recording Toolbar** to create an audio note. Can be synchronized with PC Outlook notes using ActiveSync.

Pictures and Video



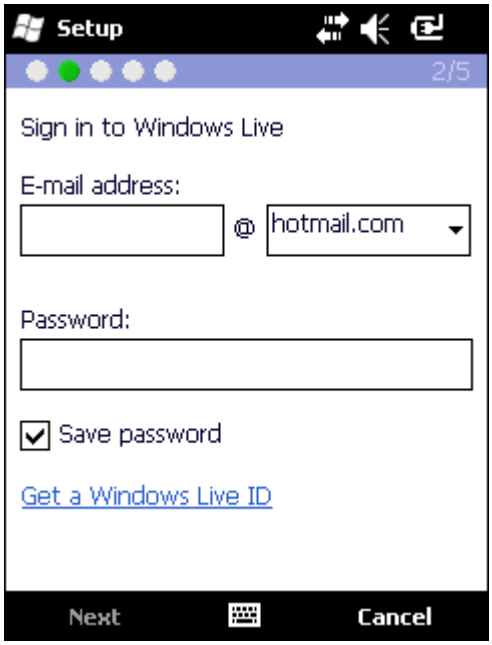
Pictures and Video. Picture/video viewer application. Can be synchronized with PC My Documents folder using ActiveSync.

Tasks



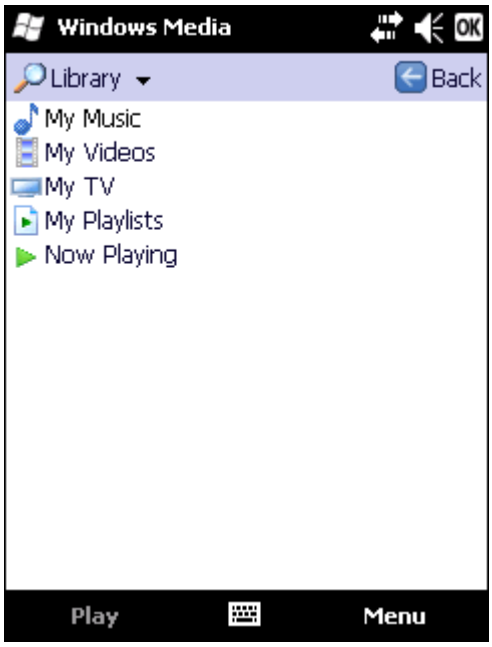
Tasks. Task list application. Can be synchronized with PC Outlook task list using ActiveSync.

Windows Live



Windows Live. Sign in to Microsoft Windows Live online service. Internet access required.

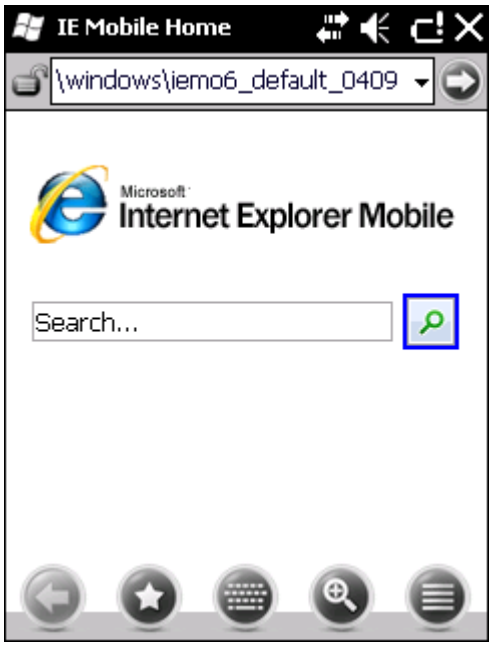
Windows Media



Windows Media. Audio visual management program. Not supported on the MX7 Tecton.

Internet Explorer Mobile

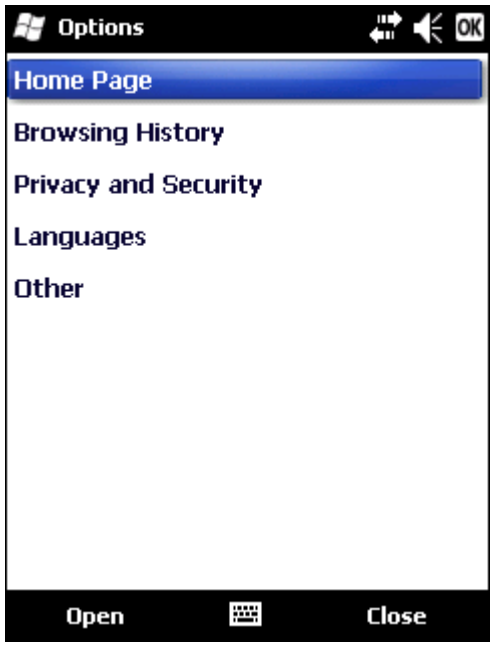
Set options for Internet connectivity. The navigation icons change state based on the web page contents.

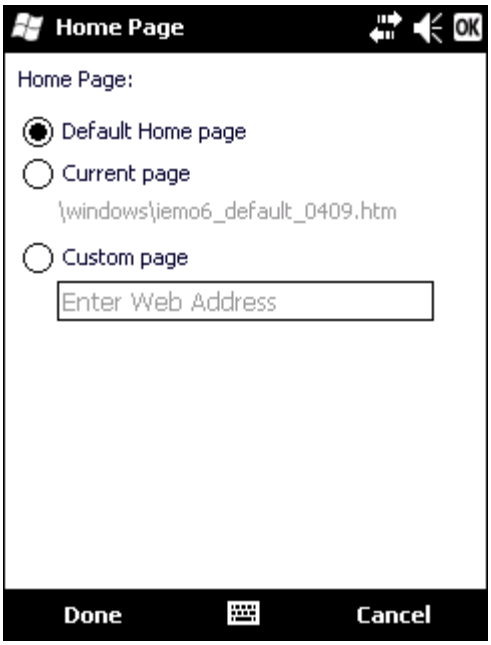


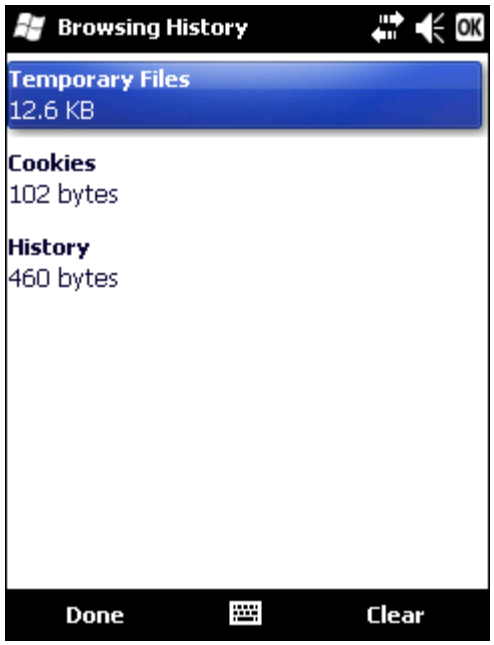
Navigation Icon	Action	Navigation Icon	Action
	Add folder		Favorites
	Add to Favorites		Options
	Go Back		Soft Input Panel
	Delete Favorite		Zoom In Zoom Out
	Edit Favorites		

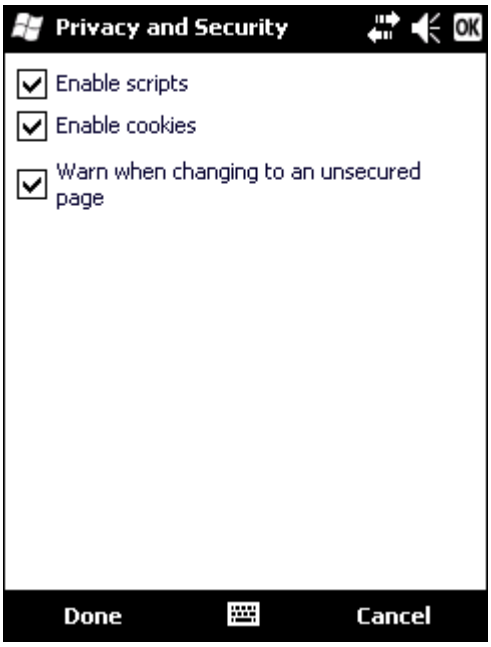
Options

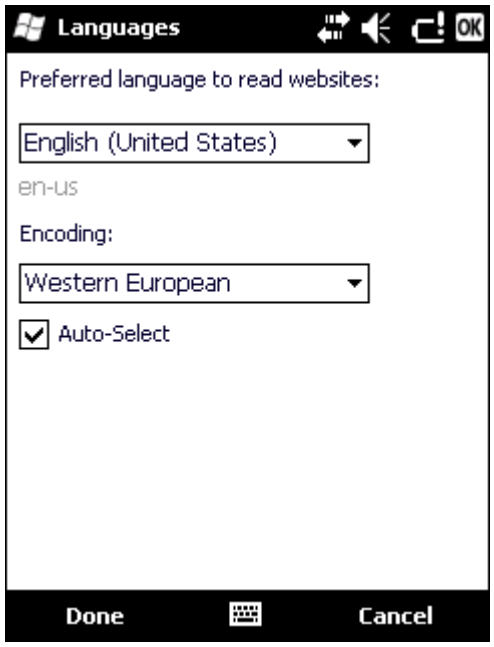

IE Mobile Hom
\windows\iemc
Microsoft
Interne
Search...
Home Page
History
Forward
Refresh
View
Tools
Copy/Paste
Exit
Send Link...
Properties
Options

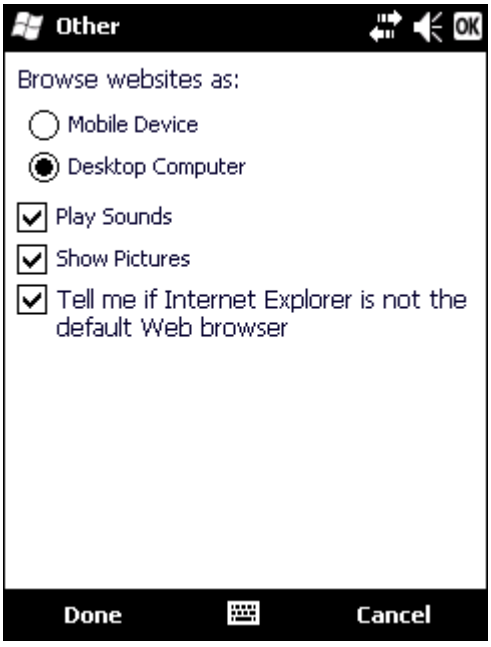

Options
Home Page
Browsing History
Privacy and Security
Languages
Other
Open
Close


Home Page
Home Page:
Default Home page
Current page
\windows\iemo6_default_0409.htm
Custom page
Enter Web Address
Done
Cancel


Browsing History
Temporary Files
12.6 KB
Cookies
102 bytes
History
460 bytes
Done
Clear


Privacy and Security
OK
Enable scripts
Enable cookies
Warn when changing to an unsecured page
Done
Cancel


Languages
OK
Preferred language to read websites:
English (United States)
en-us
Encoding:
Western European
Auto-Select
Done
Cancel


Other
OK
Browse websites as:
Mobile Device
Desktop Computer
Play Sounds
Show Pictures
Tell me if Internet Explorer is not the default Web browser
Done
Cancel

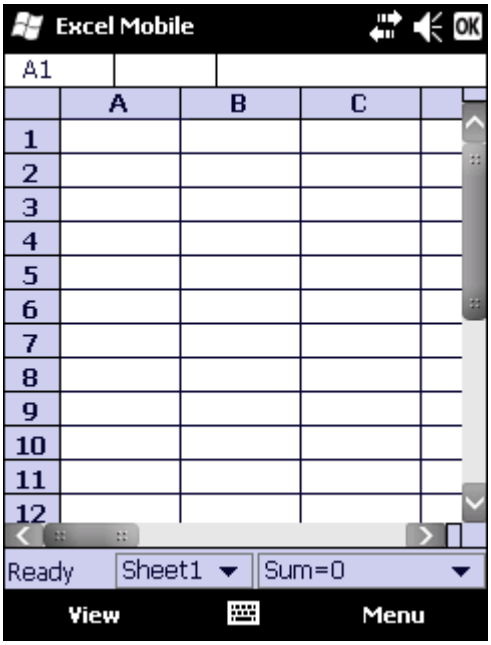
Office Mobile

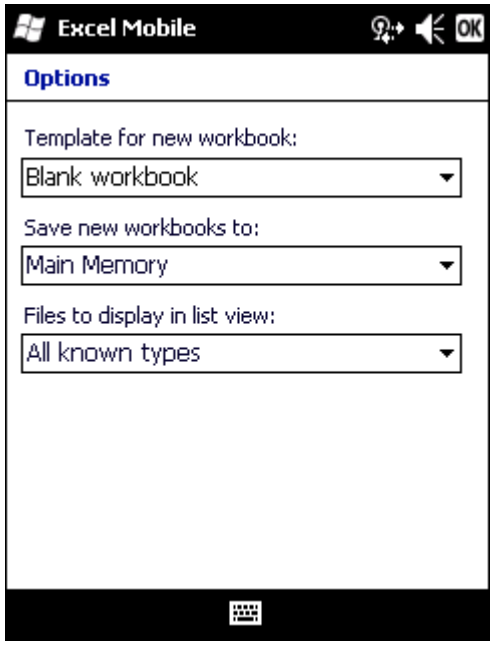
A suite of business related applications. Files can be created, opened, viewed, saved in different formats, etc.

Note: For Microsoft Office Mobile instruction for Word, PowerPoint, Excel and OneNote, refer to commercially available Microsoft Office Mobile user guides.

Excel Mobile

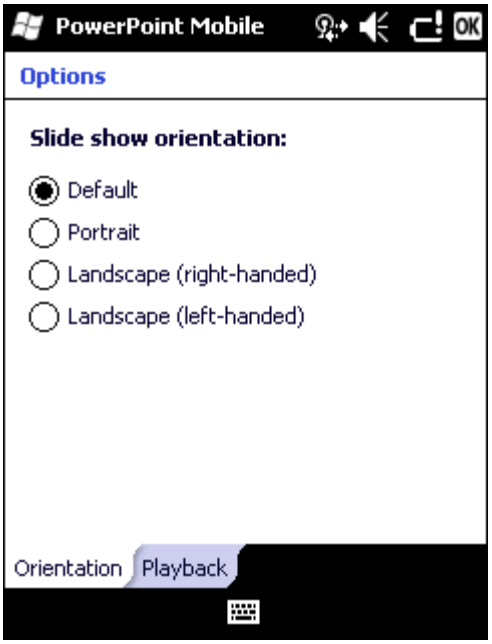
Spreadsheets can be edited, data can be sorted, formatting and changes are preserved. Select **Menu > Options** to change default settings.





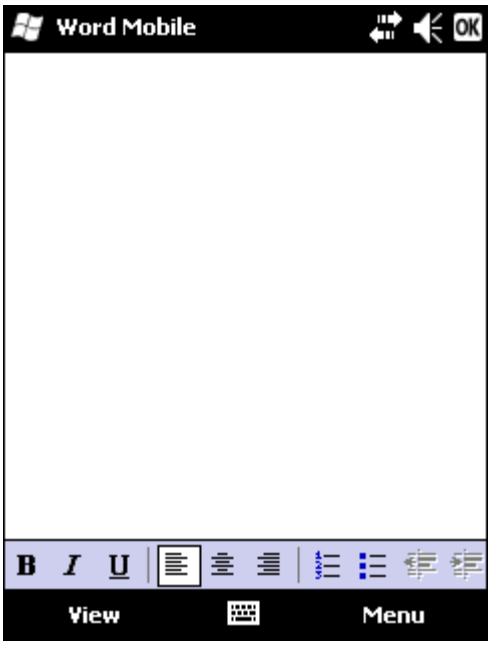
PowerPoint Mobile

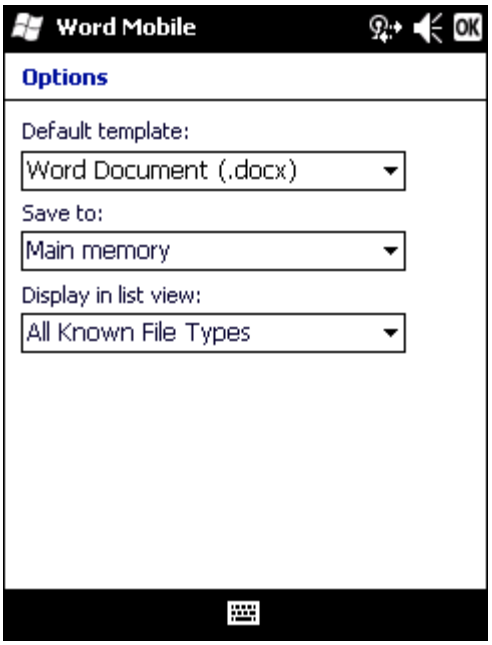
Open, view and edit slides in landscape or portrait format. Zoom and GoTo features enabled. Select **Menu > Options** to change default settings.



Word Mobile

Open, view, edit documents. Formats are saved. Spelling checker, cut and paste are available, undo and redo commands. Select **Menu > Options** to change default settings.





OneNote Mobile

OneNote is an electronic version of a paper notebook. Select Menu to change default settings.

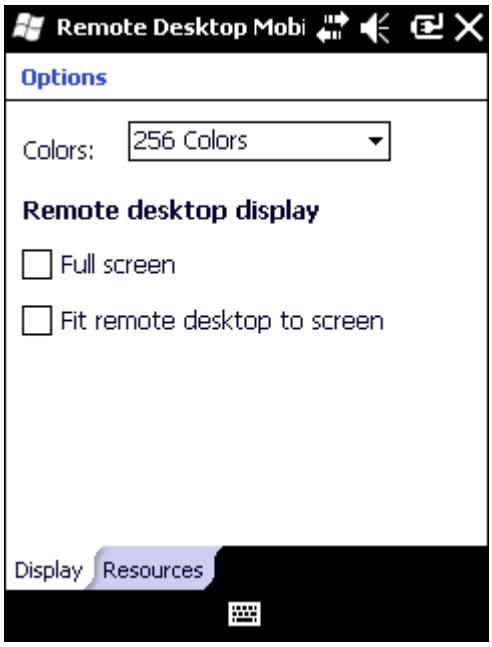
Remote Desktop

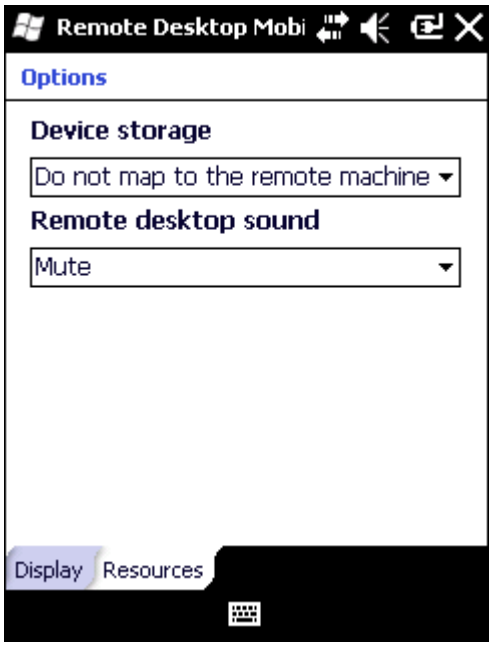
Start > Remote Desktop Mobile

Using Remote Desktop Mobile, you can log on to a remote computer running Terminal Services or Remote Desktop and use all the programs available on that computer from your mobile device. For example, instead of running Word Mobile on the MX7 Tecton, you can run the desktop computer version of Word and access all of the .doc files on that computer from your device.

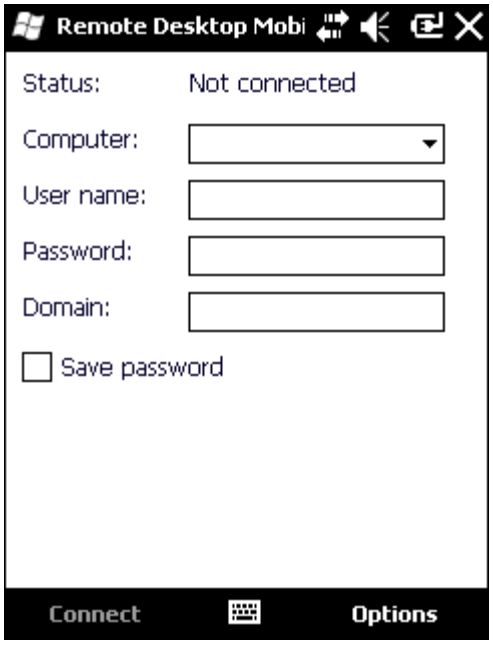
Set Remote Desktop Mobile Options

Before connecting to a remote computer, set Remote Desktop Mobile options to improve display and resource when connected, if desired. Tap Options in the taskbar. Tap OK when finished.





Connect to a Remote Server



1. Configure the radio.
2. Enter the name of the computer to which you want to connect. If needed, enter the port number at the end of the computer name (*remotecomputername*:*portnumber*).
3. Enter the user name, password and domain.
4. Tap the **Save password** check box if it is blank.
5. Tap **Connect** to complete the connection and save the password.
6. Select **Disconnect** from Remote Desktop connection.
7. Create a folder titled **Startup** under the **System** folder.
8. Copy Remote.exe from the Windows folder to the \System\Startup folder just created.
9. Select **Start > Settings > System > MX7 Tecton Options** and check **Remote Desktop Autologon**.
10. Select **OK** and **yes** to reboot.
11. Result: The unit will boot into the Remote Desktop Connection.

Installing Applications

Applications can be installed on the MX7 Tecton from CAB files or package files.

Package files have some unique characteristics:

- Package files patch the operating system so they become non-volatile. Even a Clean Boot does not remove the programs.
- CAB files are (re)installed after a cold boot, but not after a suspend/resume since the OS was not reset and the CAB files are still in use.
- Packages can contain registry settings which are installed at setup, similar to a CAB file.
- Package files cannot be uninstalled, reinstalled or reverted to an earlier version.
- Packages can be digitally signed.
- A super package file can be created containing multiple package files. Because the MX7 Tecton must reboot after every package installation, a super package may make the installation faster.
- Package files have a .PKG extension, super package files have a .PKS extension.

An unsigned executable (CAB or package file) prompts the user when executed:

The program is from an unknown publisher. Running it can possibly harm your device. Do you want to continue?

If you trust the program, tap Yes. Otherwise tap No.

Preparation

Package files can be copied to the MX7 Tecton via ActiveSync or they can be installed from the Flash card.

Package File Installation

The MX7 Tecton must be connected to external AC power. IMPORTANT – Because the package file installation actually rewrites portions of the operating system, it is important that power is not interrupted during package file installation. If power is interrupted, the operating system may be damaged, requiring the MX7 Tecton to be returned to Honeywell for repair.

Use File Explorer to browse to the location of the package file.

1. Tap the package file. Note that by default the file extension is hidden. The package file can be either a single package file or a super package file.
2. The installation process begins.
3. A Validating Update display is presented indicating that an update has been received. The device will verify the update before installing.
4. When prompted, tap Install Now to begin the installation.
5. The MX7 Tecton reboots and displays an Update message while the package is being installed.
6. When the installation is completed, the MX7 Tecton reboots again and displays the summary screen.

Refer to Help below if there is a problem with the package installation.

PKG Installation Help

Issue:

The MX7 Tecton isn't connected to AC power.

Solution:

Updates cannot be installed while the device is on battery power. To continue, connect the power adapter to the mobile device. The update will be deleted when Cancel is tapped.

Tap Cancel. Connect the MX7 Tecton to AC power and try the update again.

The message that the update will be deleted only means that the scheduled update was deleted. The package file IS NOT deleted and remains on the storage card.

Issue:

The package is already installed or is an older version than installed.

Solution:

Status unsuccessful. The update could not be installed because the update has already been installed or the package file is an earlier version than the version currently installed on the MX7 Tecton.

Tap Done to exit the update process.

The message that the update could not be installed and is deleted only means that the scheduled update was deleted. The package file IS NOT deleted and remains on the storage card.

Contact Technical Assistance (page 16-1) or your system administrator for more information on package versions.

Using ActiveSync

Introduction

Requirement : ActiveSync (version 4.5 or higher for Windows XP host computers) must be resident on the host (desktop/laptop) computer. Windows Mobile Device Center (version 6.1 or higher) is required for a Windows Vista or higher desktop/laptop computer. ActiveSync and Windows Mobile Device Center for the host computer is available from the Microsoft website. Follow their instructions to locate, download and install ActiveSync or Windows Mobile Device Center on your desktop computer.

Note: For readability in this section, ActiveSync will be used in instructions and explanations. If you have a Windows Vista or higher operating system on your host computer, replace "ActiveSync" with "Windows Mobile Device Center".

Using Microsoft ActiveSync, you can synchronize information on your host computer with the MX7 Tecton and vice versa. Synchronization compares the data on your mobile device with your host computer and updates both with the most recent data.

For example, you can:

- Back up and restore your device data.
- Copy (rather than synchronize) files between your device and host computer.
- Control when synchronization occurs by selecting a synchronization mode. For example, you can synchronize continually while connected to your host computer or only when you choose the synchronize command.

By default, ActiveSync does not automatically synchronize all types of information. Use ActiveSync Options to specify the types of information you want to synchronize. The synchronization process makes the data (in the information types you select) identical on both your host computer and your device.

When installation of ActiveSync is complete on your host computer, the ActiveSync Setup Wizard begins and starts the following processes:

- connect your MX7 Tecton to your host computer,
- set up a partnership so you can synchronize information between your mobile device and your desktop computer, and
- customize your synchronization settings.

Because ActiveSync is already installed on the MX7 Tecton, your first synchronization process begins automatically when you finish setting up your host computer in the ActiveSync wizard. For more information about using ActiveSync on your host computer, open ActiveSync, then open ActiveSync Help.

Initial Setup

The initial setup of ActiveSync must be made via a USB connection. Partnerships can only be created using USB cable connection.

Connect via USB

The default connection type is USB Client. This is the only connection option supported on the MX7 Tecton.

To verify it is set to USB, select

Start > Settings > Connections > USB to PC

Ensure the check box for “Enable advanced network functionality” is checked. Tap OK to return to the Connections panel.

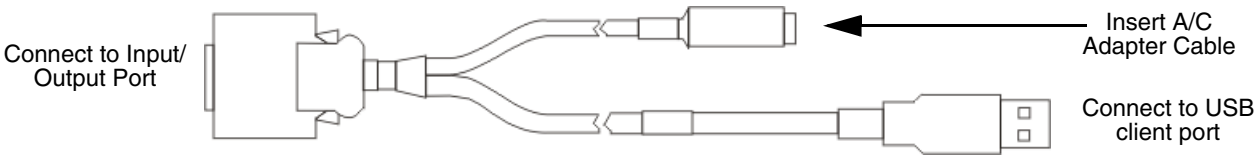
Connect the USB cable to the PC (the host) and the MX7 Tecton (the client) as detailed below. ActiveSync will start automatically when the USB cable is connected.

When the MX7 Tecton loses connection, e.g., enters Suspend Mode, etc., the connection to ActiveSync will be lost. When the MX7 Tecton resumes, the ActiveSync session will automatically re-connect.

Cable for USB ActiveSync Connection

MX7052CABLE - MX7 Tecton Charge/Comm Interface Cable with USB Client port for ActiveSync. USB end of cable connects to PC/Laptop USB port.

- Connect the MX7 Tecton end of the cable to the I/O port on the bottom of the MX7 Tecton
- The USB type A connector on the cable connects to a USB port on a PC or laptop.
- It is not necessary to connect the power connector on the cable in order to use ActiveSync.



Explore

From the ActiveSync Dialog on the Desktop PC, tap the Explore button, which allows you to explore the mobile device from the PC side, with some limitations. You can copy files to or from the mobile device by drag-and-drop. You will not be allowed to delete files or copy files out of the \Windows folder on the mobile device. (Technically, the only files you cannot delete or copy are ones marked as system files in the original build of the Windows image. This, however, includes most of the files in the \Windows folder).

Backup Data Files using ActiveSync

Use the following information to backup data files from the mobile device to a PC using the appropriate cable and ActiveSync.

Requirements

A partnership between the mobile device and ActiveSync has been established.

- A desktop or laptop PC with an available USB port and a mobile device with a USB port. The desktop or laptop PC must be running Windows XP or greater.
- Use the specific USB cable as shown above in *Connect via USB*.

Connect

Connect the USB cable to the PC (the host) and the mobile device (the client).

The “Get Connected” wizard on the host PC checks COM ports to establish a connection for the first time.

Note: USB synchronization will start automatically when the cable is connected.

Disconnect

- Disconnect the cable from the MX7 Tecton.
- Open the status bar icon in the lower right hand corner of the status bar. Then tap the Disconnect button.

When the MX7 Tecton loses connection, e.g., enters Suspend Mode, etc., the connection to ActiveSync will be lost. When the MX7 Tecton resumes, the ActiveSync session will automatically re-connect.

MX7 Tecton with a Disabled Touch Screen

A MX7 Tecton touch screen can be disabled (using the MX7 Tecton Options control panel Misc tab). In these cases, it may be easier to configure the MX7 Tecton using ActiveSync and HXM Connect (or LXEConnect) rather than using the MX7 Tecton keypad only.

Reset and Loss of Host Re-connection

ActiveSync assigns a partnership between a client and a host computer. A partnership is defined by two objects – a unique computer name and a random number generated when the partnership is first created. An ActiveSync partnership between a unique client can be established to two hosts.

When the mobile device is reset (return to default settings), the random number is deleted – and the partnership with the last one of the two hosts is also deleted. The host retains the random numbers and unique names of all devices having a partnership with it. Two clients cannot have a partnership with the same host if they have the same Device Name.

If the reset mobile device tries to reestablish the partnership with the same host PC, a new random number is generated for the mobile device and ActiveSync will insist the unique name of the mobile device be changed. If the mobile device is associated with a second host, changing the name will destroy that partnership as well. This can cause some confusion when re-establishing partnerships with hosts.

ActiveSync Help

Issue:

ActiveSync on the host says that a device is trying to connect, but it cannot identify it

Solution:

One or more control lines are not connected. This is usually a cable problem, but on a laptop or other device, it may indicate a bad serial port.

If the MX7 Tecton is connected to a PC by a cable, disconnect the cable from the MX7 Tecton and reconnect it again.

Check that the correct connection is selected.

See Also: Reset and Loss of Host Re-connection above.

Issue:

ActiveSync indicator on the host (disc in the toolbar tray) turns green and spins as soon as you connect the cable, before tapping the Connect icon.

Solution:

One or more control lines are tied together incorrectly. This is usually a cable problem, but on a laptop or other device, it may indicate a bad serial port.

Issue:

ActiveSync indicator on the host turns green and spins, but connection never occurs

Solution:

Check that the correct connection is selected.

-or-

Incorrect or broken data lines in cable.

Issue:

ActiveSync indicator on the host remains gray

Solution 1:

ActiveSync icon on the PC does not turn green after connecting USB cable from MX7 Tecton.

1. Disconnect MX7 Tecton USB cable from PC.
2. Suspend/Resume or Restart the MX7 Tecton.
3. In **ActiveSync > File > Connection Settings** on PC disable Allow USB Connections and tap **OK**.
4. Re-enable Allow USB Connections on the PC and tap **OK**.
5. Reconnect USB cable from MX7 Tecton to PC.

Solution 2:

The host doesn't know you are trying to connect. May mean a bad cable, with no control lines connected, or an incompatible baud rate. Try the connection again, with a known good cable.

Configuring the MX7 Tecton with HSM Connect (or LXEConnect)

HSM Connect (or LXEConnect) allows a user to view the MX7 Tecton screen remotely from a PC using an ActiveSync connection.

Requirements: ActiveSync (version 4.5 or higher for Windows XP host computers) must be resident on the host computer. Windows Mobile Device Center (version 6.1 or higher) is required for a Windows Vista/ or greater host computer.

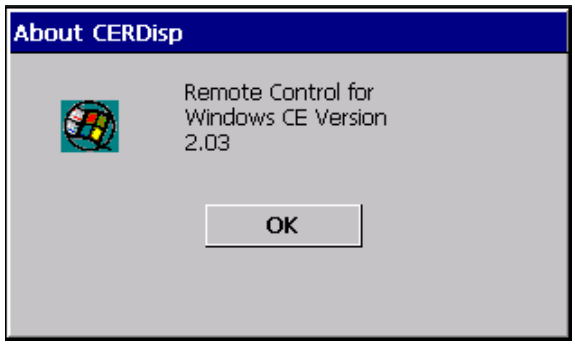
ActiveSync is already installed on the MX7 Tecton. The MX7 Tecton is pre-configured to establish a USB ActiveSync connection to a host PC when the USB cable is attached to the MX7 Tecton and the host PC.

Install HSM Connect

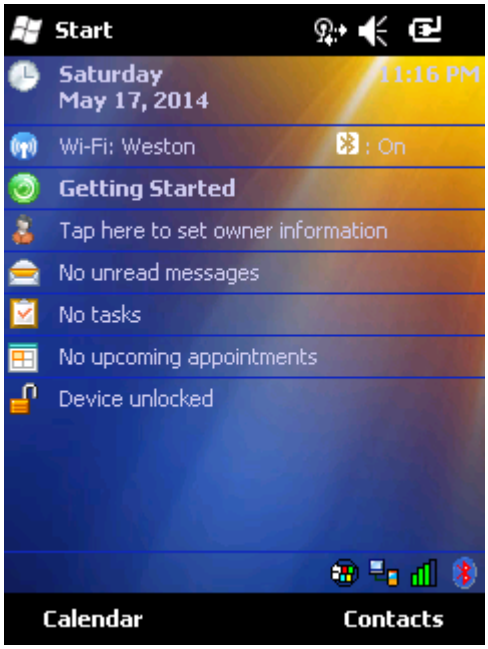
1. HSM Connect for the MX7 Tecton running Windows Mobile is available on the *Getting Started Disc*.
2. Download the files to a location on your host PC hard drive.
3. Execute the setup.exe file that was copied to the host PC. This setup program installs the HSM Connect utility.
4. Follow the on screen installation prompts.
5. When the installation is complete, create a desktop shortcut to HSM Connect.
6. HSM Connect is now installed on the host PC and ready to use.

Using HSM Connect

1. Power up the MX7 Tecton.
2. Connect the MX7 Tecton to the host PC using the USB connection cable. Once connected, the ActiveSync dialog box appears and the ActiveSync connection is automatically established.
3. Select "No" for partnership when prompted. Dismiss any ActiveSync dialog boxes warning a partnership is not set up. It is not necessary to establish a partnership to use HSM Connect. However, if a partnership is desired for other reasons, one may be established now.
4. Double-tap the HSM Connect icon that was created on the PC desktop.
5. HSM Connect launches.



6. Click the OK button to dismiss the About CERDisp dialog box on the MX7 Tecton desktop by clicking the OK button in the HSM Connect window on the PC desktop. The dialog box automatically times out and disappears after approximately 20 seconds.



7. The MX7 Tecton can now be configured from the HSM Connect window. Input from the PC's mouse and keyboard are recognized as if they were attached to the MX7 Tecton.

8. When the remote session is completed, terminate the HSM Connect program by selecting **File > Exit** or clicking on the X in the upper right hand corner to close the application, then disconnect the ActiveSync cable.

6

AppLock (Application Locking)

Introduction

AppLock is designed to be run on Windows based devices only. The AppLock program is factory installed.

Configuration parameters are specified by the AppLock Administrator for the MX7 Tecton end user. AppLock is password protected by the Administrator.

End user mode locks the end user into the configured application or applications. The end user can still reboot the mobile device and respond to dialog boxes. The administrator-specified applications are automatically launched in the specified order and run in full screen mode when the MX7 Tecton boots up.

When the mobile device is reset to factory default values, for example after a cold reset, the Administrator may need to configure the AppLock parameters again.

The assumption, in this chapter, is that the first user to power up a new mobile device is the system administrator.

MX7 Tecton AppLock is setup by the Administrator by tapping **Start > Settings > System > Administration** icon.

Note: AppLock Administrator panel file Launch option does not inter-relate with similarly-named options contained in other MX7 Tecton System Panels.

Note: A few applications do not follow normal procedures when closing. AppLock cannot prevent this type of application from closing, but is notified that the application has closed. For these applications, AppLock immediately restarts the application (see Auto Re-Launch) which causes the screen to flicker. If this type of application is being locked, the administrator should close all other applications before switching to end user mode to minimize the screen flicker.

Setup a New Device

Prerequisites:

- A default input method (Input Panel, Transcriber, or custom input method) is assigned.

Devices with AppLock are shipped to boot in Administration mode with no default password, thus when the device is first booted, the user has full access to the MX7 Tecton and no password prompt is displayed. After the administrator specifies applications to lock, assigns passwords and the device is rebooted or the hotkey is pressed, the MX7 Tecton switches to end user mode.

The process to configure a new device using AppLock is as follows:

1. Insert a fully charged battery and press the Power button.
2. Connect an external power source to the device (if required).
3. Adjust screen display, audio volume and other parameters if desired. Install accessories (e.g., handstrap, stylus) if needed.
4. Tap **Start > Settings > System > Administration** control panel.
5. Assign a Switch Key (Hot Key) sequence for AppLock on the Security (page 6-9).
6. Assign an application on the Application (page 6-5). More than one application can be assigned.
7. Assign a password on the Security panel.
8. Select a view level on the Status (page 6-11), if desired.
9. Tap **OK**.
10. Press the Switch Key sequence to launch AppLock and lock the configured application(s). The device is now in end user mode.

Administration Mode

Administration mode gives full access to the mobile device, hardware and software configuration options.

The administrator must enter a valid password (when a password has already been assigned) before access to Administration mode and configuration options are allowed. The administrator can configure the following options:

- Create/change the keystroke sequence to activate administrator access.

- Create/change the password for administrator access.
- Assign the name of the application, or applications, to lock.
- Select the command line of the application to lock.

In addition to these configuration options, the administrator can view and manage the status logs of AppLock sessions.

Administrator default values for this device are:

- Administrator Hotkey - Shift+Ctrl+A
- Password - none
- Application path and name - none
- Application command line - none

End User Mode

The default end user Hotkey Activation key is Ctrl+Spc.

End user mode locks the end user into the configured application or applications. The end user can still reboot and respond to dialog boxes. Each application is automatically launched and runs in full screen mode when the device boots up.

The end user cannot unintentionally or intentionally exit the application nor can the end user execute any other applications. Normal application exit or switching methods and all Microsoft defined Windows OS key combinations, such as close (X) icon, File Exit, File Close, Alt-F4, Alt-Tab, etc. are disabled. The Windows OS desktop icons, menu bars, task bar and system trays are not visible or accessible. Task Manager is not available.

If the end user selects File/Exit or Close from the application menu bar, the menu is cleared and nothing else happens; the application remains active. Nothing happens when the end user clicks on the Close icon on the application's title bar and the application remains active.

Note: A few applications do not follow normal procedures when closing. AppLock cannot prevent this type of application from closing, but is notified that the application has closed. For these applications, AppLock immediately restarts the application which causes the screen to flicker. If this type of application is being locked, the administrator should close all other applications before switching to end user mode to minimize the screen flicker.

Windows accelerator keys such as Alt-F4 are disabled.

Passwords

A password must be configured. If the password is not configured, a new device switches into Administration mode without prompting for a password. In addition to the Administrator hotkey press, a mode switch occurs if inaccurate information has been configured or if mandatory information is missing in the configuration.

There are several situations that display a password prompt after a password has been configured.

If the configured hotkey is pressed, the password prompt is displayed. In this case the user has 30 seconds (and within three attempts) to enter a password. If a valid password is not entered within 30 seconds, the password prompt is dismissed and the device returns to end user mode.

All other situations that present the password prompt do not dismiss the prompt -- this is because the other situations result in invalid end user operation.

These conditions include:

- If inaccurate configuration information is entered by the administrator, i.e., an application is specified that does not exist.
- If the application name, which is mandatory for end user mode, is missing in the configuration.
- Invalid installation of AppLock (e.g., missing DLLs).
- Corrupted registry settings.

To summarize, if an error occurs that prevents AppLock from switching to end user mode, the password will not timeout and AppLock will wait until the correct password is entered.

AppLock Password Help

Contact ***Technical Assistance*** (page 16-1) when troubleshooting passwords.

End-User Switching Technique

The default end user Hotkey Activation key is Ctrl+Spc..

Switchpad Menu

A check mark indicates applications currently active or available for Launching by the user. When Keyboard is selected, the MX7 Tecton default input method (Input Panel, Transcriber, or custom input method) is activated.

The check mark to the left of the application name indicates that the application is active.

If the application is listed but does not have a check mark to the left of the application name, this means the application is configured in AppLock and can be manually launched by tapping on the application name in the list.

Using a Stylus Tap

When the mobile device enters end user mode, a Switchpad icon (it looks like three tiny windows one above the other) is displayed in the lower right corner of the display. The Switchpad is always visible on top of the application in focus. However, if only one application is configured in AppLock and the Input Panel is disabled the Switchpad is not visible.

When the user taps the Switchpad icon, a menu is displayed showing the applications available to the user. The user can tap an application name in the popup menu and the selected application is brought to the foreground. The previous application continues to run in the background. Stylus taps affect the application in focus only. When the user needs to use the Input Panel, they tap the Keyboard option. Input Panel taps affect the application in focus only.

Using the Switch Key Sequence

One switch key sequence (or hotkey) is defined by the administrator for the end user to use when switching between locked applications. This is known as the **Activation key**. The Activation key is assigned by the Administrator using the Global Key setting in the Application panel.

When the switch key sequence is pressed on the keypad, the next application in the AppLock configuration is moved to the foreground (in focus) and the previous application moves to the background. The previous application continues to run in the background. End user key presses affect the application in focus only.

Hotkey (Activation hotkey)

If the MX7 Tecton has been configured to use AppLock to allow the user to switch between applications, the default user Activation key is **Ctrl+Spc**. The key sequence switches the focus between one application and another. Data entry affects the application running in the foreground only. Note that the system administrator may have assigned a different key sequence to use when switching applications.

End User Internet Explorer (EUIE)

AppLock supports applications that utilize Internet Explorer, such as HTML pages and JAVA applications. The end user can run an application by entering the application name and path in Internet Explorer's address bar.

To prevent the end user from executing an application using this method, the address bar and Options settings dialog are restricted in Internet Explorer. This is accomplished by creating an Internet Explorer that is used in end user mode: End user Internet Explorer (EUIE.EXE). The EUIE executes the Internet Explorer application in full screen mode which removes the address bar and status bar. The Options Dialog is also removed so the end user cannot re-enable the address bar.

The administrator specifies the EUIE by tapping the Internet check box in the Application tab of the Administrator applet. The internet application should then be entered in the Application text box.

When the Internet check box is enabled, the Menu and Status check boxes are available.

Enabling the Menu check box displays the EUIE menu which contains navigation functions like Back, Forward, Home, Refresh, etc., functions that are familiar to most Internet Explorer users. When the Menu check box is blank, the EUIE menu is not displayed and Navigation functions are unavailable.

When the Status check box is enabled, the status bar displayed by EUIE gives feedback to the end user when they are navigating the Internet.

If the standard Internet Explorer that is shipped with the mobile device is desired, it should be treated like any other application. This means that IEXPLORER.EXE (or equivalent) should be specified in the Application text box and the internet application should be entered in the command line. In this case, do not check the Internet check box.

Application Configuration

The default Administrator Hotkey sequence is **Shift+Ctrl+A**.

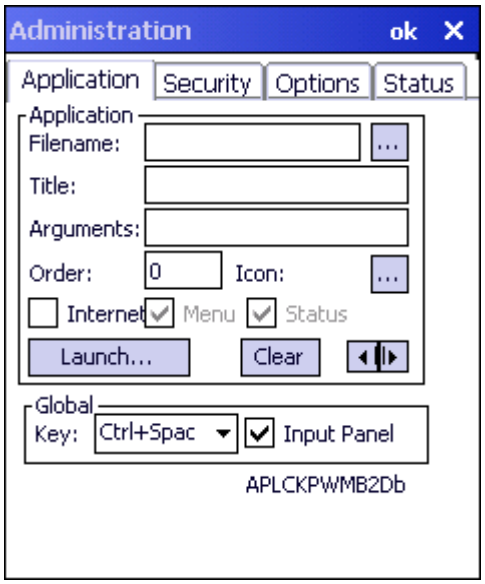
Administrator mode allows access to all features on the device. When the hotkey is pressed to switch into Administrator mode, a password prompt is displayed (if a password has been configured). A password must be entered within 30 seconds (and within three tries) or the password prompt is removed and the device remains in end user mode with the focus returned to the locked application. Without entry of a valid password, the switch into Administrator mode will not occur.

The password prompt is displayed if a password has been configured. When the valid password is entered, the Administration panel is displayed. When a valid password is not entered within 30 seconds, the user is returned to the System Panel.

If a password has not been configured, the Administrator panel is displayed.

Note: Before setting up multiple instances of the same application, make sure the targeted software application will allow two instances to run at the same time.

Application



Use the Application tab options to select the applications to launch when the device boots up in End user Mode.

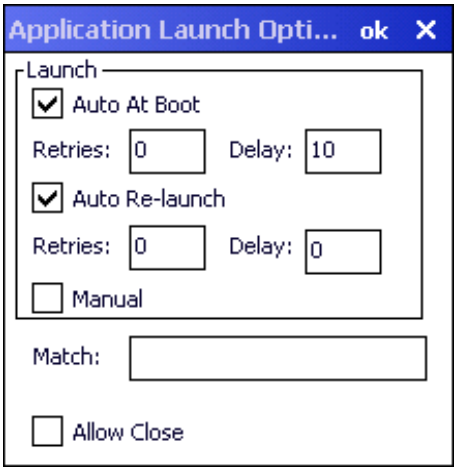
If no application is specified when the Administrator Panel is closed, the MX7 Tecton reboots into Administrator mode. If a password has been set, but an application has not been specified, the user will be prompted for the password before entering administration mode. The password prompt remains on the display until a valid password is entered.

Setting	Function
Filename	Default is blank. Move the cursor to the Filename text box and either type the application path or tap the Browse button (the … button). The standard Windows Browse dialog is displayed. After selecting the application from the Browse dialog, tap **OK**.
Title	Default is blank. Enter the Title to be associated with the application. The assumption is that multiple copies of the same application may need unique titles in order to differentiate them in the Switchpad.
Arguments	Default is blank. Enter the command line parameters for the application in the Arguments text box.
Order	Default is 1. Enter the Order in which the application is to be loaded or presented to the end user. Applications are launched in lowest to highest number order and do not need to be sequential.
Internet	Default is Disabled. Tap the Internet check box to enable the End user Internet Explorer (EUIE.EXE) When the check box is enabled, the Internet Menu and Internet Status are available. See the section titled End User Internet Explorer (EUIE) (page 6-4) for more details.
Launch Button	See following section titled Launch Button (page 6-7).

Setting	Function
Global Key	Default is Ctrl+Spc. Select the Global Key key sequence the end user is to press when switching between applications. The Global Key default key sequence must be defined by the AppLock Administrator. The Global key is presented to the end user as the Activation key.
Global Delay	Default is 10 seconds. Enter the number of seconds that Applications must wait before starting to run after reboot. *Note: Delay (Global) may not be available in all versions of AppLock. You can simulate a Global Delay function by setting a delay for the first application (lowest Order) launched and setting the delay to 0 for all other applications.*
Input Panel	Default is Disabled. Enable (check) to show the Keyboard option on the Switchpad menu. When enabled the input panel cannot be enabled or disabled for each individual application, and is available to the user for all configured applications.
Clear Button	Tap the Clear button to clear all currently displayed Filename or Application information. The Global settings are not cleared.
Scroll Buttons	Use the left and right scroll buttons to move from application setup screen to application setup screen. The left and right buttons update the information on the screen with the previous or next configured application respectively.

Launch Button

When clicked, displays the Launch options panel for the Filename selected on the Administration panel.



Note: Launch order is determined by the Order specified in the Application panel. The Order value does not have to be sequential.

Auto At Boot

Default is Enabled.

When enabled, automatically launches (subject to the specified Delay in seconds) the application after the unit is rebooted. If a Delay in seconds is specified, AppLock waits for the specified period of time to expire before launching the application. The Delay default value is 10 seconds; valid values are between 0 “no delay” and a maximum of 999 seconds.

Retries

This is the number of times the application launch will be retried if a failure occurs when the application is automatically launched at bootup. Valid values are between 0 (no tries) and 99 tries or -1 for infinite. Infinite tries ends when the application successfully launches. The default is 0 retries.

Delay

This timer is the time that AppLock waits prior to the initial launch of the selected application when it is automatically launched at bootup. Delay default is 10 seconds. Valid values are between 0 seconds (no delay) and 999 seconds.

The Auto At Boot delay is associated for each application; it will be either a value specified by the Administrator or it will be the delay default value. At startup, when a delay has been assigned for each application, AppLock waits for the delay associated with the first application to expire before launching the first application then AppLock waits for the delay associated with the second application to expire before launching the second application. AppLock continues in this manner until all applications are launched.

Note: A “Global Delay” can be accomplished by setting a timed delay for the first application to be launched (by lowest Order number) and no delay (0 seconds) for all other applications.

Note: Launch order is determined by the Order specified in the Application tab. The Order value does not have to be sequential.

Auto Re-Launch

Default is Enabled.

When enabled for a specific application. automatically re-launches it (subject to the specified Auto Re-Launch Delay in seconds) after it terminates. This option allows the Administrator to disable the re-launch operation. AppLock cannot prevent all applications from closing. When an application that AppLock cannot prevent from closing terminates, perhaps because of an error condition, AppLock re-launches the application when this option is enabled.

Note: If Allow close (page 6-8) is enabled and both Auto Re-launch and Manual (Launch) are disabled, the application cannot be restarted for the end user or by the end user after the application terminates.

Retries

Default is 0 tries. Retries is the number of times AppLock will try to re-launch the application. The retry count is reset after an application is successfully launched and controlled by AppLock. Valid values are between 0 (no tries) and 99 tries or -1 for infinite. Infinite tries ends when the application successfully launches.

Delay

Default is 0 seconds (no delay). Delay is the amount of time AppLock waits prior to re-launching an application that has terminated. The delay is specified in seconds. Valid values are between 0 (no delay) and 99 seconds.

AppLock must also be configured to automatically re-launch an application. To AppLock, application termination by the end user is indistinguishable from application termination for any other reason.

Manual (Launch)

Default is Disabled.

Enabling this option allows the end user to launch the specified application(s). Upon bootup completion an application with Manual enabled is listed on the Switchpad accompanied by a checkmark that indicates the application is currently active or available for Launching. When an application name is tapped by the end user, the application is launched (if inactive) and brought to the foreground.

Applications set up with Manual (Launch) enabled may or may not be launched at bootup. This function is based on the application's Auto At Boot setting. The applications have been listed as approved applications for end user manual launch using the Switchpad menu structure. The approved applications are listed on the Switchpad. A checkmark indicates the applications active status.

When Manual (Launch) is disabled for an application, and Allow Close is enabled for the application, when the end user closes the specific application it is no longer available (shown) on the Switchpad.

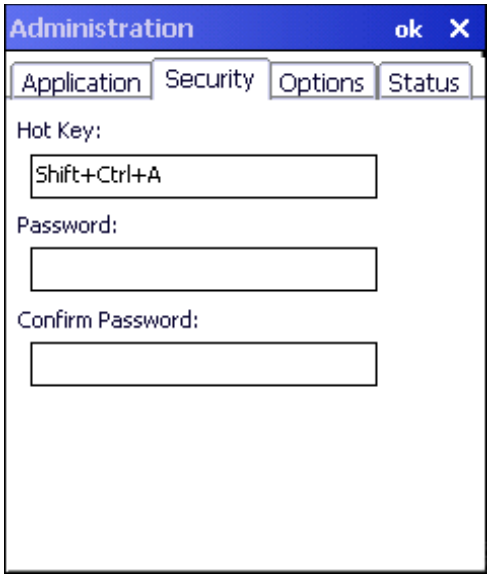
When Auto At Boot and Manual (Launch) are both disabled for a specific application, the application is 1) not placed on the list of approved applications for end user manual launch and 2) never launched, and 3) not displayed on the Switchpad.

Allow close

Default is Disabled. When enabled, the associated application can be closed by the end user.

This option allows the administrator to configure applications that consume system resources to be terminated if an error condition occurs or at the end user's request. Error conditions may generate a topmost popup requiring an end user response, memory resource issues requiring an end user response, etc. Also at the administrator's discretion, these types of applications can be started manually (see Manual [Launch]) by the end user.

Security



Setting an Activation Hotkey

Specify the hotkey sequence that triggers AppLock to switch between administrator and user modes and the password required to enter Administrator mode. The default hotkey sequence is Shift+Ctrl+A.

A 2nd key keypress is an invalid keypress for a hotkey sequence.

Move the cursor to the Hot Key text box. Enter the new hot key sequence by first pressing the Shift state key followed by a normal key. The hotkey selected must be a key sequence that the application being locked does not use. The hot-key sequence is intercepted by AppLock and is not passed to the application.

Input from the keyboard or Input Panel is accepted with the restriction that the normal key must be pressed from the keyboard when switching modes. The hotkey sequence is displayed in the Hot key text box with <Shift>, <Alt>, and <Ctrl> text strings representing the shift state keys. The normal keyboard key completes the hotkey sequence. The hotkey must be entered via the keypad. Some hotkeys cannot be entered via the Input Panel. Also, hotkeys entered via the SIP (Soft Input Panel) are not guaranteed to work properly when switching operational modes.

For example, if the <Ctrl> key is pressed followed by <A>, Ctrl+A is entered in the text box. If another key is pressed after a normal key press, the hotkey sequence is cleared and a new hotkey sequence is started.

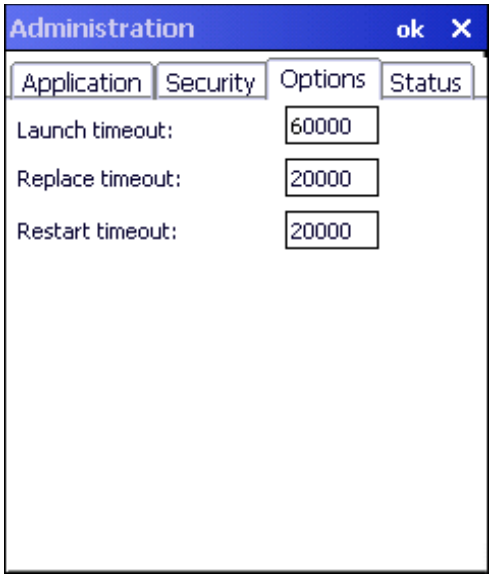
A normal key is required for the hotkey sequence and is unlike pressing the normal key during a mode switch; this key can be entered from the SIP when configuring the key. However, when the hotkey is pressed to switch user modes, the normal key must be entered from the keypad; it cannot be entered from the SIP.

Setting a Password in the Security Panel

Move the cursor to the Password text box. The passwords entered in the Password and Confirm Password fields must match. Passwords are case sensitive.

When the user exits the Administrator panel, the two passwords are compared to verify that they match. If they do not match, a dialog box is displayed notifying the user of the error. After the user closes the dialog box, the Security Panel is displayed and the password can then be entered and confirmed again. If the passwords match, the password is encrypted and saved.

Options



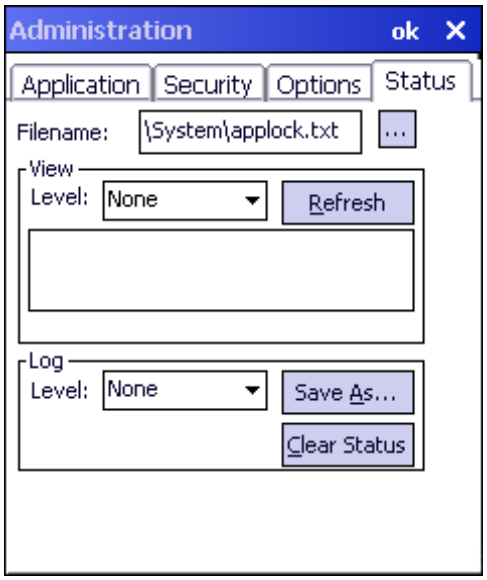
AppLock uses 3 timeout values when locking applications:

Setting	Explanation
Launch timeout	The time to wait for an application to initially launch before timing out. Default value is 60000 milliseconds (60 seconds).
Replace timeout	The time to wait for an application to replace the current window with another one before timing out. Default value is 20000 milliseconds (20 seconds).
Restart timeoutt	The time to wait for an application to restart itself before timing out. Default value is 20000 milliseconds (20 seconds).

Status

Use the Status panel to view the log of previous AppLock operations and to configure which messages are to be recorded during AppLock operation.

Status information is stored in a specific location on the storage device and in a specific logfile specified by the Administrator. For this reason, the administrator can configure the type of status information that is logged, as well as clear the status information.



Move the cursor to the Filename text box and either type the logfile path or tap the Browse button (the … button). The standard Windows OS Browse dialog is displayed. After selecting the logfile from the Browse dialog, tap **OK**.

View

Setting	Explanation
Error	Error status messages are logged when an error occurs and is intended to be used by the administrator to determine why the specified application cannot be locked.
Process	Processing status shows the flow control of AppLock components and is mainly intended for Customer Support when helping users troubleshoot problems with their AppLock program.
Extended	Extended status provides more detailed information than that logged by Process Logging.
All	All messages are displayed.

Tap the Refresh button after changing from one view level to another. The filtered records are displayed, all others are not displayed.

Log

Note: If a level higher than Error is selected, the status should be cleared frequently by the administrator.

In addition to the three view levels the administrator can select that all status information be logged or turn off all status information logging completely. The system default is 'None'; however to reduce registry use, the administrator may want to select 'None' after verifying the configuration. Tap the Clear button to clear the status information from the registry.

- None
- Error
- Processing
- Extended
- All

Save As

When the 'Save As'… button is selected, a standard 'Save As' dialog screen is displayed. Specify the path and filename. If the filename exists, the user is prompted whether the file should be overwritten. If the file does not exist, it is created.

AppLock Help

Issue:

The MX7 Tecton won't switch from Administration mode to end user mode.

Solution:

- If the configuration is valid for one application but not the other, the switch to end user mode fails. AppLock stays in Administration mode and is paused until the Administrator password is entered.
- If two copies of the same application are configured, but the application only allows one copy to run at a time, for example Microsoft Pocket Word and RFTerm, the switch to end user fails. AppLock stays in Administration mode and is paused until the Administrator password is entered.

Issue:

The hotkey sequence needed is not allowed. What does this mean?

Solution:

When the Administrator is selecting a hotkey sequence to use when switching user modes, they are not allowed to enter key combinations that are reserved by installed software applications. Honeywell has validated RFTerm key combinations ONLY.

When RFTerm is installed on the mobile device and an RFTerm restricted key sequence is specified as a hotkey sequence by the Administrator, the following error message is displayed in a message box:

Selected hotkey is not allowed. Please reenter.

When RFTerm is not installed on the mobile device, the RFTerm keys are not restricted from use.

Issue:

Can't locate the password that has been set by the administrator?

Solution:

Contact Technical Assistance (page 16-1) for administrator password help.

AppLock Error Messages

Any messages whose first word is an 'ing' word is output prior to the action described in the message. For example, "Switching to admin-hotkey press" is logged after the administrator has pressed the hotkey but prior to starting the switch process.

For all operations that can result in an error, an Error level message is displayed when a failure occurs. These messages contain the word "failure". These messages have a partner Extended level message that is logged which contains the word "**OK**" if the action completed successfully rather than with an error.

For processing level messages, "Enter…" is logged at the beginning of the function specified in the message and "Exit…" is logged at the end (just before the return) of the function specified in the message.

Message	Explanation and/or corrective action	Level
Error reading hotkey	The hotkey is read but not required by AppLock.	LOG_EX
Error reading hotkey; using default	A hotkey is required. If there is a failure reading the hotkey, the internal factory default is used.	LOG_ERROR
App Command Line= <Command line>	Command line of the application being locked	LOG_PROCESSING
App= <Application name>	Name of the application being locked	LOG_PROCESSING
dwProcessID= <#>	Device ID of the application being locked	LOG_EX
Encrypt exported key len <#>	Size of encrypt export key	LOG_EX
Encrypt password length= <#>	The length of the encrypted password.	LOG_EX
Encrypted data len <#>	Length of the encrypted password	LOG_EX
hProcess= <#>	Handle of the application being locked	LOG_EX
Key pressed = <#>	A key has been pressed and trapped by the hotkey processing.	LOG_EX
**********	The status information is being saved to a file and the file has been opened successfully.	LOG_EX
Address of keyboard hook procedure failure	AppLock found the kbdhook.dll, but was unable to get the address of the initialization procedure. For some reason the dll is corrupted. Look in the \Windows directory for kbdhook.dll. If it exists, delete it. Also delete AppLock.exe from the \Windows directory and reboot the unit. Deleting AppLock.exe triggers the AppLock system to reload.	LOG_ERROR
Address of keyboard hook procedure OK	AppLock successfully retrieved the address of the keyboard filter initialization procedure.	LOG_EX
Alt pressed	The Alt key has been pressed and trapped by the HotKey processing.	LOG_EX
Alt	Processing the hotkey and backdoor entry	LOG_EX
Application handle search failure	The application being locked did not complete initialization.	LOG_ERROR
Application handle search OK	The application initialized itself successfully	LOG_ERROR
Application load failure	The application could not be launched by AppLock; the application could not be found or is corrupted.	LOG_ERROR
Backdoor message received	The backdoor keys have been pressed. The backdoor hotkeys provide a method for customer service to get a user back into their system without editing the registry or reloading the device.	LOG_PROCESSING
Cannot find kbdhook.dll	The load of the keyboard filter failed. This occurs when the dll is missing or is corrupted. Look in the \Windows directory for kbdhook.dll. If it exists, delete it. Also delete AppLock.exe from the \Windows directory and reboot the unit. Deleting AppLock.exe triggers the AppLock system to reload.	LOG_ERROR
Converted Pwd	Converted password from wide to mbs.	LOG_EX

Message	Explanation and/or corrective action	Level
Could not create event EVT_HOTKEYCHG	The keyboard filter uses this event at the Administrator Control panel. The event could not be created.	LOG_ERROR
Could not hook keyboard	If the keyboard cannot be controlled, AppLock cannot process the hotkey. This failure prevents a mode switch into user mode.	LOG_ERROR
Could not start thread HotKeyMon	The keyboard filter must watch for hot key changes. The watch process could not be initiated.	LOG_ERROR
Ctrl after L or X	Processing the backdoor entry.	LOG_EX
Ctrl pressed	The Ctrl key has been pressed and trapped by the HotKey processing.	LOG_EX
Ctrl	Processing the hotkey and backdoor entry.	LOG_EX
Decrypt acquire context failure	Unable to decrypt password.	LOG_ERROR
Decrypt acquired context OK	Decryption process ok.	LOG_EX
Decrypt create hash failure	Unable to decrypt password.	LOG_ERROR
Decrypt created hash OK	Decryption process ok.	LOG_EX
Decrypt failure	Unable to decrypt password.	LOG_ERROR
Decrypt import key failure	Unable to decrypt password.	LOG_ERROR
Decrypt imported key OK	Decryption process ok.	LOG_EX
Encrypt acquire context failure	Unable to encrypt password.	LOG_ERROR
Encrypt acquire encrypt context failure	Unable to encrypt password.	LOG_ERROR
Encrypt acquired encrypt context OK	Encrypt password process successful.	LOG_EX
Encrypt create hash failure	Unable to encrypt password.	LOG_ERROR
Encrypt create key failure	Unable to encrypt password.	LOG_ERROR
Encrypt created encrypt hash OK	Encrypt password process successful.	LOG_EX
Encrypt export key failure	Unable to encrypt password.	LOG_ERROR
Encrypt export key length failure	Unable to encrypt password.	LOG_ERROR
Encrypt exported key OK	Encrypt password process successful.	LOG_EX
Encrypt failure	The password encryption failed.	LOG_ERROR
Encrypt gen key failure	Unable to encrypt password.	LOG_ERROR
Encrypt generate key failure	Unable to encrypt password.	LOG_ERROR
Encrypt get user key failure	Unable to encrypt password.	LOG_ERROR
Encrypt get user key ok	Encrypt password process successful.	LOG_EX

Message	Explanation and/or corrective action	Level
Encrypt hash data failure	Unable to encrypt password.	LOG_ERROR
Encrypt hash data from pwd OK	Encrypt password process successful.	LOG_EX
Encrypt length failure	Unable to encrypt password.	LOG_ERROR
Encrypt out of memory for key	Unable to encrypt password.	LOG_ERROR
Encrypted data OK	The password has been successfully encrypted.	LOG_EX
Enter AppLockEnum-Windows	In order for AppLock to control the application being locked so it can prevent the application from exiting, AppLock launches the application and has to wait until it has created and initialized its main window. This message is logged when the function that waits for the application initialization is entered.	LOG_EX
Enter DecryptPwd	Entering the password decryption process.	LOG_PROCESSING
Enter EncryptPwd	Entering the password encryption processing.	LOG_PROCESSING
Enter FullScreenMode	Entering the function that switches the screen mode. In full screen mode, the taskbar is hidden and disabled.	LOG_PROCESSING
Enter GetAppInfo	Processing is at the beginning of the function that retrieves the application information from the registry.	LOG_PROCESSING
Enter password dialog	Entering the password dialog processing.	LOG_PROCESSING
Enter password timeout	Entering the password timeout processing.	LOG_PROCESSING
Enter restart app timer	Some application shut down before AppLock can stop it. In these cases, AppLock gets notification of the exit. When the notification is received, AppLock starts a timer to restart the application. This message logs that the timer has expired and the processing is at the beginning of the timer function.	LOG_PROCESSING
Enter TaskbarScreen-Mode	Entering the function that switches the screen to non-full screen mode and enable the taskbar.	LOG_PROCESSING
Enter ToAdmin	Entering the function that handles a mode switch into admin mode.	LOG_PROCESSING
Enter ToUser	Entering the function that handles the mode switch to user mode	LOG_PROCESSING
Enter verify password	Entering the password verification processing.	LOG_PROCESSING
Exit AppLockEnum-Windows-Found	There are two exit paths from the enumeration function. This message denotes the enumeration function found the application.	LOG_PROCESSING
Exit AppLockEnum-Windows-Not found	There are two exit paths from the enumeration function. This message denotes the enumeration function did not find the application.	LOG_PROCESSING
Exit DecryptPwd	Exiting password decryption processing.	LOG_PROCESSING
Exit EncryptPwd	Exiting password encryption processing.	LOG_PROCESSING
Exit FullScreenMode	Exiting the function that switches the screen to full screen.	LOG_PROCESSING
Exit GetAppInfo	Processing is at the end of the function that retrieved the application information from the registry.	LOG_PROCESSING
Exit password dialog	Exiting password prompt processing.	LOG_PROCESSING
Exit password dialog-cancel	Exiting password prompt w/cancel.	LOG_PROCESSING
Exit password dialog-OK	Exiting password prompt successfully.	LOG_PROCESSING
Exit password timeout	Exiting password timeout processing.	LOG_PROCESSING
Exit restart app timer	Processing is at the end of the timer function	LOG_PROCESSING
Exit TaskbarScreen-Mode	Exiting the function that switches the screen mode back to normal operation for the administrator.	LOG_PROCESSING

Message	Explanation and/or corrective action	Level
Exit ToAdmin	Exiting the function that handles the mode switch into admin mode.	LOG_PROCESSING
Exit ToUser	Exiting the user mode switch function.	LOG_PROCESSING
Exit ToUser-Registry read failure	The AppName value does not exist in the registry so user mode cannot be entered.	LOG_PROCESSING
Exit verify password-no pwd set	Exiting password verification.	LOG_PROCESSING
Exit verify password-response from dialog	Exiting password verification.	LOG_PROCESSING
Found taskbar	The handle to the taskbar has been found so that AppLock can disable it in user mode.	LOG_PROCESSING
Getting address of keyboard hook init procedure	AppLock is retrieving the address of the keyboard hook.	LOG_PROCESSING
Getting configuration from registry	The AppLock configuration is being read from the registry. This occurs at initialization and also at entry into user mode. The registry must be re-read at entry into user mode in case the administration changed the settings of the application being controlled.	LOG_PROCESSING
Getting encrypt pwd length	The length of the encrypted password is being calculated.	LOG_EX
Hook wndproc failure	AppLock is unable to lock the application. This could happen if the application being locked encountered an error after performing its initialization and shut itself down prior to being locked by AppLock.	LOG_ERROR
Hook wndproc of open app failure	The application is open, but AppLock cannot lock it.	LOG_ERROR
Hot key event creation failure	The Admin applet is unable to create the hotkey notification.	LOG_ERROR
Hot key pressed	Processing the hotkey and backdoor entry	LOG_EX
Hot key pressed	Processing the hotkey and backdoor entry	LOG_EX
Hot key set event failure	When the administrator changes the hotkey configuration the hotkey controller must be notified. This notification failed.	LOG_ERROR
Hotkey press message received	The user just pressed the configured hotkey.	LOG_PROCESSING
In app hook:WM_SIZE	In addition to preventing the locked application from exiting, AppLock must also prevent the application from enabling the taskbar and resizing the application's window. This message traps a change in the window size and corrects it.	LOG_EX
In app hook:WM_WINDOWPOSCHANGED	In addition to preventing the locked application from exiting, AppLock must also prevent the application from enabling the taskbar and resizing the application's window. This message traps a change in the window position and corrects it.	LOG_EX
Initializing keyboard hook procedure	AppLock is calling the keyboard hook initialization.	LOG_PROCESSING
Keyboard hook initialization failure	The keyboard filter initialization failed.	LOG_ERROR
Keyboard hook loaded OK	The keyboard hook dll exists and loaded successfully.	LOG_EX
L after Ctrl	Processing the backdoor entry.	LOG_EX
Loading keyboard hook	When AppLock first loads, it loads a dll that contains the keyboard hook processing. This message is logged prior to the load attempt.	LOG_PROCESSING
Open failure	The status information is being saved to a file and the file open has failed. This could occur if the file is write protected. If the file does not exist, it is created.	LOG_ERROR
Open registry failure	If the Administration registry key does not exist, the switch to user mode fails because the AppName value in the Administration key is not available.	LOG_ERROR

Message	Explanation and/or corrective action	Level
Opened status file	The status information is being saved to a file and the file has been opened successfully.	LOG_EX
Out of memory for encrypted pwd	Not enough memory to encrypt the password.	LOG_ERROR
pRealTaskbarWndProc already set	The taskbar control has already been installed.	LOG_EX
Pwd cancelled or invalid-remain in user mode	The password prompt was cancelled by the user or the maximum number of failed attempts to enter a password was exceeded.	LOG_EX
Read registry error-hot key	The hotkey registry entry is missing or empty. This is not considered an error. The keyboard hook uses an embedded default if the value is not set in the registry.	LOG_ERROR
Read registry failure-app name	AppName registry value does not exist or is empty. This constitutes a failure for switching into user mode.	LOG_ERROR
Read registry failure-Cmd Line	AppCommandLine registry entry is missing or empty. This is not considered an error since command line information is not necessary to launch and lock the application.	LOG_ERROR
Read registry failure-Internet	The Internet registry entry is missing or empty. This is not considered an error since the Internet value is not necessary to launch and lock the application.	LOG_ERROR
Registering Backdoor MSG	The AppLock system communicates with the keyboard hook via a user defined message. Both AppLock.exe and Kbdhook.dll register the message at initialization.	LOG_PROCESSING
Registering Hotkey MSG	The AppLock system communicates with the keyboard hook via a user defined message. Both Applock.exe and Kbdhook.dll register the message at initialization.	LOG_PROCESSING
Registry read failure at reenter user mode	The registry has to be read when entering user mode is the AppName is missing. This user mode entry is attempted at boot and after a hotkey switch when the administrator has closed the application being locked or has changed the application name or command line.	LOG_ERROR
Registry read failure at reenter user mode	The registry has to be read when switching into user mode. This is because the administrator can change the settings during administration mode. The read of the registry failed which means the Administration key was not found or the AppName value was missing or empty.	LOG_ERROR
Registry read failure	The registry read failed. The registry information read when this message is logged is the application information. It the Administration key cannot be opened or if the AppName value is missing or empty, this error is logged. The other application information is not required. If the AppName value is not available, AppLock cannot switch into user mode.	LOG_ERROR
Reset system work area failure	The system work area is adjusted when in user mode to cover the taskbar area. The system work area has to be adjusted to exclude the taskbar area in administration mode. AppLock was unable to adjust this area.	LOG_ERROR
Shift pressed	The Shift key has been pressed and trapped by the HotKey processing.	LOG_EX
Shift	Processing the hotkey and backdoor entry	LOG_EX
Show taskbar	The taskbar is now being made visible and enabled.	LOG_PROCESSING
Switching to admin-backdoor	The system is currently in user mode and is now switching to admin mode. The switch occurred because of the backdoor key presses were entered by the administrator.	LOG_PROCESSING
Switching to admin-hotkey press	The system is currently in user mode and is now switching to admin mode. The switch occurred because of a hotkey press by the administrator.	LOG_PROCESSING
Switching to admin-kbdhook.dll not found	The keyboard hook load failed, so AppLock switches to admin mode. If a password is specified, the password prompt is displayed and remains until a valid password is entered.	LOG_PROCESSING
Switching to admin-keyboard hook initialization failure	If the keyboard hook initialization fails, AppLock switches to admin mode. If a password is specified, the password prompt is displayed and remains until a valid password is entered.	LOG_PROCESSING

Message	Explanation and/or corrective action	Level
Switching to admin-registry read failure	See the explanation of the “Registry read failure” above. AppLock is switching into Admin mode. If a password has been configured, the prompt will be displayed and will not be dismissed until a valid password is entered.	LOG_PROCESSING
Switching to Taskbar-ScreenMode	In administration mode, the taskbar is visible and enabled.	LOG_EX
Switching to user mode	The registry was successfully read and AppLock is starting the process to switch to user mode.	LOG_PROCESSING
Switching to user-hot-key press	The system is currently in admin mode and is now switching to user mode. The switch occurred because of a hotkey press by the administrator.	LOG_PROCESSING
Taskbar hook failure	AppLock is unable to control the taskbar to prevent the locked application from re-enabling it.	LOG_ERROR
Taskbar hook OK	AppLock successfully installed control of the taskbar.	LOG_EX
Timeout looking for app window	After the application is launched, AppLock must wait until the application has initialized itself before proceeding. The application did not start successfully and AppLock has timed out.	LOG_ERROR
ToUser after admin, not at boot	The user mode switch is attempted when the device boots and after the administrator presses the hotkey. The mode switch is being attempted after a hotkey press.	LOG_EX
ToUser after admin-app still open	The switch to user mode is being made via a hotkey press and the administrator has left the application open and has not made any changes in the configuration.	LOG_EX
ToUser after admin-no app or cmd line change	If user mode is being entered via a hotkey press, the administrator may have left the configured application open. If so, AppLock does not launch the application again unless a new application or command line has been specified; otherwise, it just locks it.	LOG_EX
Unable to move desktop	The desktop is moved when switching into user mode. This prevents them from being visible if the application is exited and restarted by the timer. This error does not affect the screen mode switch; processing continues.	LOG_ERROR
Unable to move taskbar	The taskbar is moved when switching into user mode. This prevents them from being visible if the application is exited and restarted by the timer. This error does not affect the screen mode switch; processing continues.	LOG_ERROR
Unhook taskbar wndproc failure	AppLock could not remove its control of the taskbar. This error does not affect AppLock processing	LOG_ERROR
Unhook wndproc failure	AppLock could not remove the hook that allows monitoring of the application.	LOG_ERROR
Unhooking taskbar	In administration mode, the taskbar should return to normal operation, so AppLock’s control of the taskbar should be removed.	LOG_EX
Unhooking wndproc	When the administrator leaves user mode, the device is fully operational; therefore, AppLock must stop monitoring the locked application.	LOG_EX
WM_SIZE adjusted	This message denotes that AppLock has readjusted the window size.	LOG_EX
X after Ctrl+L	Processing the backdoor entry.	LOG_EX
Ret from password <#>	Return value from password dialog.	LOG_EX
Decrypt data len <#>	Length of decrypted password.	LOG_EX
Window handle to enumwindows=%x	The window handle that is passed to the enumeration function. This message can be used by engineering with other development tools to trouble shoot application lock failures.	LOG_EX
WM_WINDOW-POSCHG adjusted=%x	Output the window size after it has been adjusted by AppLock	LOG_EX

7 Bluetooth Configuration

Introduction

Contact Technical Assistance (page 16-1) for upgrade availability if your Bluetooth panels are not the same as the panels presented in this section.

Discover and manage pairing with nearby Bluetooth devices.

Setting	Default
Discovered Devices	None
Settings	
Turn On Bluetooth	Disabled / default is Off
Computer is connectable	Enabled
Computer is discoverable	Disabled
Prompt if devices request to pair	Enabled
Continuous search	Disabled
Filtered Mode	Enabled
Printer Port on COM9:	Disabled (unchecked) by default in both Filtered and Non Filtered Modes. The option is dimmed in Non Filtered Mode.
Logging	Disabled
Computer Friendly Name	[*System Name*]
Reconnect	
Report lost connection	Enabled
Report when reconnected	Disabled
Report failure to reconnect	Enabled
Clear Pairing Table on boot	Disabled
Auto Reconnect on Boot	Enabled
Auto Reconnect	Enabled

MX7 Tecton Bluetooth client icon state and paired Bluetooth device icon states change as Bluetooth devices are discovered, paired, connected and disconnected. There may be audible or visual signals as paired devices re-connect with the MX7 Tecton.

- The default Bluetooth setting is Off.
- The MX7 Tecton cannot be discovered by other Bluetooth devices when the *Computer is discoverable* option is disabled (unchecked) on the Settings panel.
- Other Bluetooth devices cannot be discovered if they have been set up to be Non-Discoverable or Invisible.
- When Filtered Mode is enabled, the MX7 Tecton can pair with one Bluetooth scanner and one Bluetooth printer.
- When Filtered Mode is disabled, the MX7 Tecton can pair with up to four Bluetooth devices connected at the same time.
- It is not necessary to disconnect a paired scanner and printer before a different scanner or printer is paired with the MX7 Tecton.
- The target Bluetooth device should be as close as possible (up to 32.8 ft/10 meters Line of Sight) to the MX7 Tecton during the pairing process.

Assumption: The System Administrator has Discovered and Paired targeted Bluetooth devices for the MX7 Tecton. The MX7 Tecton operating system has been upgraded to the revision level required for Bluetooth client operation. An application (or API) is available that will accept data from serial Bluetooth devices.

Initial Configuration

1. Open the Bluetooth control panel or tap the Bluetooth icon.
2. Tap the Settings (page 7-6) Tab.

3. Change the Computer Friendly Name at the bottom of the Settings display. The Bluetooth MX7 Tecton default name is determined by the factory installed software version. Honeywell strongly urges assigning every MX7 Tecton a unique name (up to 32 characters) before Bluetooth Discovery is initiated.
4. Tap or uncheck the MX7 Tecton Bluetooth options on the Settings tab and the Reconnect (page 7-8) tab.
5. Tap the **OK** button to save your changes.

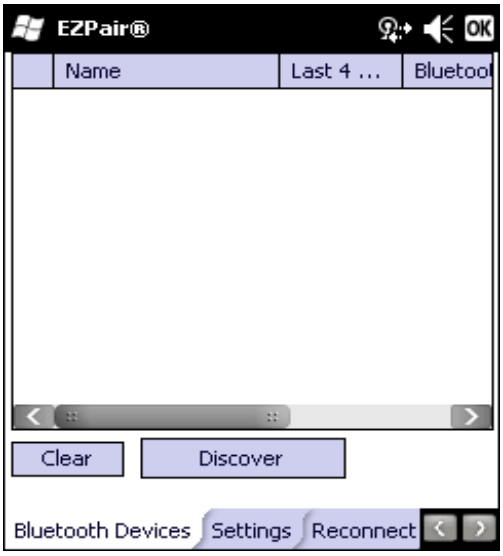
Subsequent Use

Note: MX7 Tecton Bluetooth client icon and Bluetooth device icon states change as Bluetooth devices are discovered, paired, connected and disconnected. A Bluetooth client icon with a red background indicates Bluetooth is active and not paired with any device. A device icon with a red background indicates a disconnected paired device.

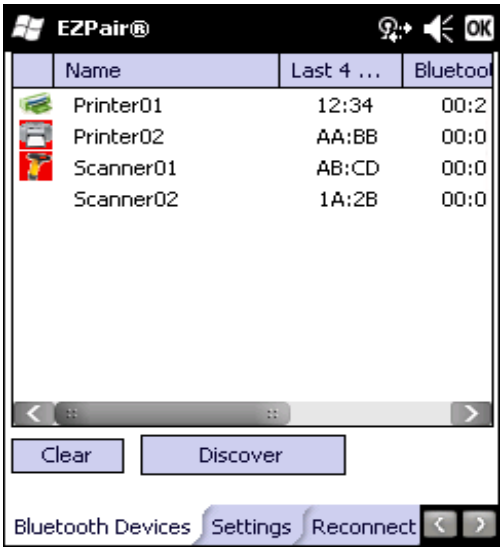
1. Tap the Bluetooth client icon to open the Bluetooth EZPair (or LXEZ Pairing) application.
2. Tap the Bluetooth Devices tab.
3. Tap the Discover button. When the Bluetooth client begins searching for in-range Bluetooth devices, the button name changes to Stop. Tap the Stop button to cancel the Discover function at any time.
4. The discovered devices are listed in the Bluetooth Devices window.
5. Highlight a Bluetooth device in the Discovered window and double-tap to open the device properties menu.
6. Tap Pair as Scanner to set up the MX7 Tecton to receive scanner data.
7. Tap Pair as Printer to set up the MX7 Tecton to send data to the printer.
8. Tap Serial Device (when Filtered mode is disabled) to set up the MX7 Tecton to communicate with a Bluetooth serial device.
9. Tap Disconnect to stop pairing with the device. Once disconnected, tap Clear to remove the device name and data from the MX7 Tecton Bluetooth Devices list. Select Yes at the *Delete all disconnected devices? Yes / No* dialog box.
10. Upon successful pairing, the selected device may react to indicate a successful connection. The reaction may be an audio signal from the device, flashing LED on the device, or a dialog box is placed on the MX7 Tecton display.
11. Whenever the MX7 Tecton is turned On, all previously paired, live, Bluetooth devices in the vicinity are paired, one at a time, with the MX7 Tecton. If the devices cannot connect to the MX7 Tecton before the re-connect timeout time period expires (default is approximately 20 seconds for each paired device) there is no indication of the continuing disconnect state if *Report Failure to Reconnect* is disabled.

Bluetooth Devices

The Bluetooth Devices tab displays any device previously discovered and paired with the MX7 Tecton.



Before Discovery



After Discovery

Clear Button

Deletes all devices from the Device table that are not currently paired. A dialog box is presented *Delete all disconnected devices?*

Tap the Yes button to remove disconnected or deleted devices from the device table. The devices are removed from the Device table after any reboot sequence and when EZPair (or LXEZ Pairing) is re-launched without rebooting. Tap the No button to make no changes.

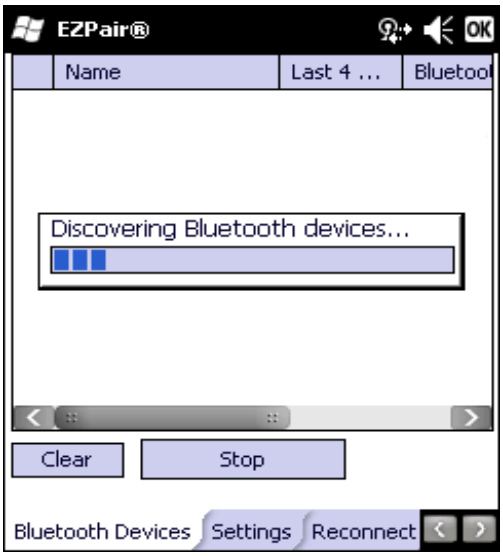
Discover Button

When tapped, the Bluetooth client discovers and displays all Bluetooth devices in the vicinity. Bluetooth managed devices should be as close as possible in direct line of sight, with the MX7 Tecton during the Discover process.

At the end of the Discover process, and when Filtered Mode is disabled/unchecked, serial Bluetooth devices as well as Bluetooth scanners and printers are displayed in the Device table. When Filtered Mode is enabled/checked, only Bluetooth scanners and printers are displayed in the Device table.

Discovering

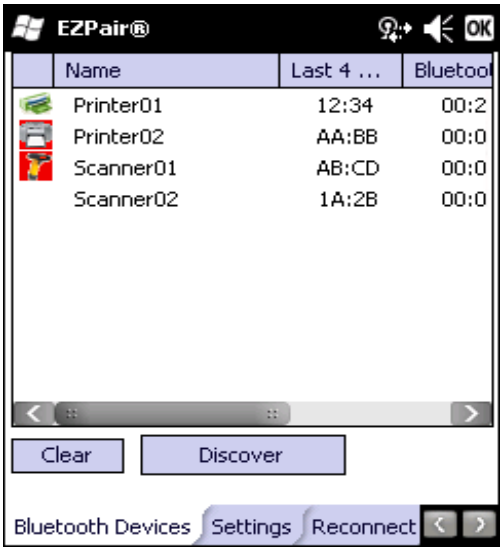
1. Tap the Discover button to locate all discoverable Bluetooth devices in the vicinity. The Discovery process also queries for the unique identifier of each device discovered.



2. Tap the Stop Button at any time to end the Discover and Query for Unique Identifier functions. The Bluetooth Device List is displayed.

Note: When an active paired device enters Suspend Mode, is turned Off or leaves the MX7 Tecton Bluetooth scanning range, the Bluetooth connection between the paired device and the MX7 Tecton is lost. There may be audible or visual signals as paired devices disconnect from the MX7 Tecton.

Bluetooth Device List



The discovered paired devices may or may not be identified with an icon. Discovered devices without an icon can be paired as a Serial device, Scanner or a Printer. The Bluetooth panel assigns an icon to the device name.

An icon with a red background indicates the device's Bluetooth connection is inactive.

An icon with a white background indicates the device is connected to the MX7 Tecton and the device's Bluetooth connection is active.

Double-tap a device in the list to open the device properties menu. The target device does not need to be active.

Bluetooth Device Menu

1. After the Discover button has been tapped and there are devices listed, tap on a device in the list to highlight it.
2. Double-tap the highlighted device to display the Bluetooth Device right click menu. The Bluetooth device does not need to be active.

Filtered Mode On

Filtered Mode Off

Right Click Menu Options

Pair as Scanner

Receive data from the highlighted Bluetooth scanner or Bluetooth imager.

Pair as Printer

Send data to the highlighted Bluetooth printer.

Pair as Serial Device

Communicate with the highlighted serial Bluetooth device. This option is available when Filtered Mode is disabled.

Disconnect

Stop the connection between the MX7 Tecton and the highlighted paired Bluetooth device.

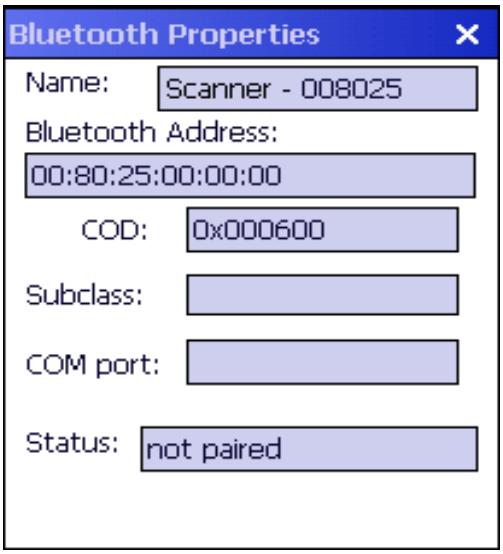
Delete

Remove an unpaired device from the Bluetooth device list. The highlighted device name and identifier is removed from the MX7 Tecton Bluetooth Devices panel after the user taps **OK**.

Properties

View more information on the highlighted Bluetooth device.

Bluetooth Properties

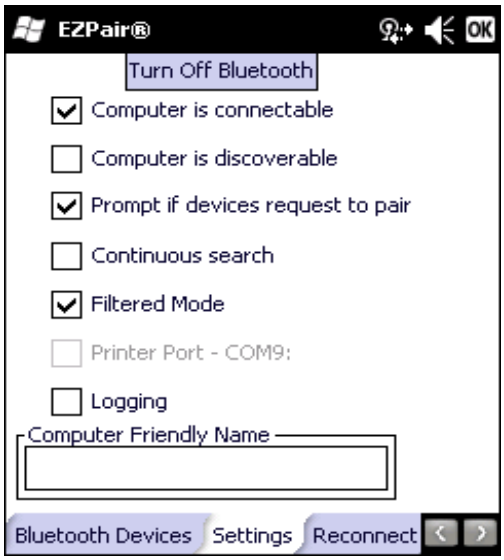


Data on the Bluetooth Properties panel cannot be changed by the user. The data displayed is the result of the device Query performed during the Discovery process.

The Status dialog box reflects the current state of the highlighted device.

Settings

Note: These options can still be checked or unchecked whether Bluetooth connection is enabled or disabled.



Turn On Bluetooth Button

Tap the button to toggle the Bluetooth client On or Off. The button title changes from *Turn Off Bluetooth* to *Turn On Bluetooth*.

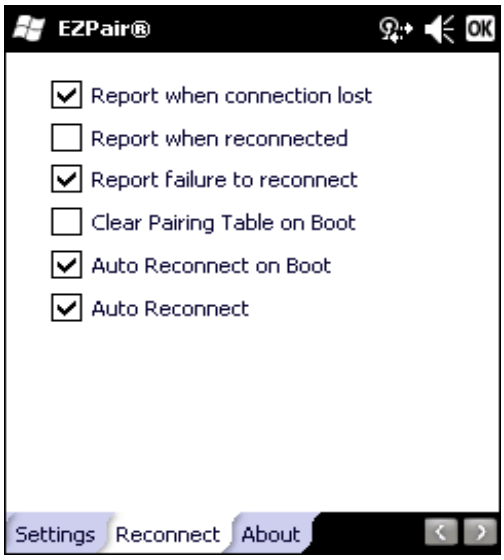
The default value is Disabled (Bluetooth client is Off).

Options

Option	Function
Computer is connectable	This option is Enabled (checked) by default. Disable this option to inhibit MX7 Tecton connection initiated by a Bluetooth scanner.
Computer is discoverable	This option is Disabled (unchecked) by default. Enable this option to ensure other devices can discover the MX7 Tecton.
Prompt if devices request to pair	This option is Enabled (checked) by default. A dialog box appears on the MX7 Tecton screen notifying the user a Bluetooth device requests to pair with the MX7 Tecton. The requesting Bluetooth device does not need to have been Discovered by the MX7 Tecton before the pairing request is received. Tap the Accept button or the Decline button to remove the dialog box from the screen. In some cases, if a Bluetooth device is already paired this setting cannot be changed. If this is the case, an error message is displayed and the option is not changed. The Bluetooth device must be disconnected before changing this setting.
Continuous Search	This option is Disabled (unchecked) by default. When enabled (checked), the Bluetooth connection never stops searching for a device it has paired with when the connection is broken (such as the paired device entering Suspend mode, going out of range or being turned off). When disabled, after being enabled, the MX7 Tecton stops searching after 30 minutes. This option draws power from the Main Battery.
Filtered Mode	This option is Enabled (checked) by default. Determines whether the Bluetooth client discovers and displays all serial Bluetooth devices in the vicinity (Filtered Mode is disabled/unchecked) or the discovery result displays Bluetooth scanners and printers only (Filtered Mode is enabled/checked). When Filtered Mode is disabled, the MX7 Tecton can pair with up to four Bluetooth devices. A Restart is required every time Filtered Mode is toggled on and off.
Printer Port - COM9	This option is Disabled (unchecked) by default. This option assigns Bluetooth printer connection to COM9 instead of COM19. To enable this option, Filtered Mode must be enabled/checked.
Logging	This option is Disabled (unchecked) by default. When logging is enabled, the MX7 Tecton creates bt_log.txt and stores it in the /System folder. Bluetooth activity logging is added to the text file as activity progresses. A bt_log_bak.txt file contains the data stored by bt_log.txt prior to reboot. During a reboot process, the MX7 Tecton renames bt_log.txt to bt_log_bak.txt. If a file already exists with that name, the existing file is deleted, the new bt_log_bak.txt file is added and a new bt_log.txt is created.
Computer Friendly Name	The name, or identifier, entered in this space by the System Administrator is used exclusively by Bluetooth devices and during Bluetooth communication.

Reconnect

Note: These options can still be checked or unchecked whether Bluetooth connection is enabled or disabled.

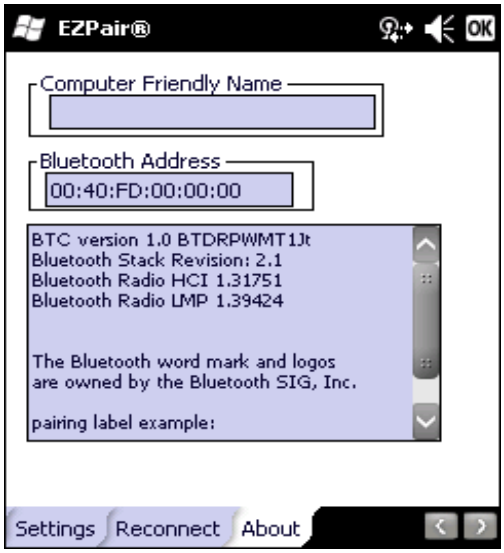


Options

Option	Function
Report when connection lost	This option is Enabled (checked) by default. There may be an audio or visual signal when a connection between a paired, active device is lost. A visual signal may be a dialog box placed on the display notifying the user the connection between one (or all) of the paired Bluetooth devices has stopped. Tap the OK button to remove the dialog box from the screen.
Report when reconnected	This option is Disabled (unchecked) by default. There may be an audio or visual signal when a connection between a paired, active device is made. A visual signal may be a dialog box placed on the display notifying the user the connection between one (or all) of the paired Bluetooth devices has resumed. Tap the ok button to remove the dialog box from the screen.
Report failure to reconnect	This option is Enabled (checked) by default. The default time delay is 30 minutes. This value cannot be changed by the user. There may be an audio or visual signal when a connection between a paired, active device fails to re-connect. A visual signal may be a dialog box placed on the display notifying the user the connection between one (or all) of the previously paired Bluetooth devices has failed. Tap the X button or ok button to close the dialog box. Possible reasons for failure to reconnect: Timeout expired without reconnecting; attempted to pair with a device that is currently paired with another device; attempted to pair with a known device that moved out of range or was turned off; attempted to pair with a known device but the reason why reconnect failed is unknown.
Clear Pairing Table on Boot	This option is Disabled (unchecked) by default. When enabled (checked), all previous paired information is deleted upon any reboot sequence and no devices are reconnected. When enabled (checked) Auto Reconnect on Boot is automatically disabled (dimmed).
Auto Reconnect on Boot	This option is Enabled (checked) by default. All previously paired devices are reconnected upon any reboot sequence. When disabled (unchecked), no devices are reconnected upon any reboot sequence.

Option	Function
Auto Reconnect	This option is Enabled (checked) by default. This option controls the overall mobile Bluetooth device reconnect behavior. When Auto Reconnect is disabled (unchecked), Auto Reconnect on Boot is automatically disabled and dimmed. When Auto Reconnect is disabled (unchecked), no devices are reconnected in any situation. The status of Auto Reconnect on Boot is ignored and no devices are reconnected on boot. The status of Clear Pairing Table on Boot controls whether the pairing table is populated on boot. When Auto Reconnect is enabled (checked) and Auto Reconnect on Boot is disabled (unchecked), devices are not reconnected on boot, but are reconnected in other situations (example: return from out-of-range). When Auto Reconnect is enabled (checked) and Clear Pairing Table on Boot is enabled (checked), devices are not reconnected on boot, but are reconnected in other situations (example: return from out-of-range). The pairing table is cleared on boot. The status of Auto Reconnect on Boot is ignored and the option is automatically disabled (unchecked) and dimmed.

About



This panel lists the pre-assigned Computer Friendly Name (that other devices may discover during their Discovery and Query process), the Bluetooth client MAC address, and software version levels. The data cannot be edited by the user.

Easy Pairing and Auto-Reconnect

The Bluetooth module can establish relationships with new devices after the user taps the Discover button. It can auto-reconnect to devices previously known but which have gone out of range and then returned within range.

Note: Configuration elements are persistent and stored in the registry.

Setup the Bluetooth module to establish how the user is notified by easy pairing and auto-reconnect events.

AppLock, if installed, does not stop the end-user from using the Bluetooth application, nor does it stop other Bluetooth-enabled devices from pairing with the MX7 Tecton while AppLock is in control.

Bluetooth Indicators

The Bluetooth icon state changes as Bluetooth devices are discovered, paired, connected and disconnected.

There may be audible or visual signals as paired devices re-connect with the MX7 Tecton.

Taskbar Icon	Legend
	MX7 Tecton is connected to one or more of the targeted Bluetooth device(s).
	MX7 Tecton is not connected to any Bluetooth device. MX7 Tecton is ready to connect with any Bluetooth device. MX7 Tecton is out of range of all paired Bluetooth device(s). Connection is inactive.

Note: When an active paired device enters Suspend Mode, is turned Off or leaves the MX7 Tecton Bluetooth scan range, the Bluetooth connection between the paired device and the MX7 Tecton is lost. There may be audible or visual signals as paired devices disconnect from the MX7 Tecton.

AppLock, if installed, does not stop the end-user from using Bluetooth applications, nor does it stop authorized Bluetooth-enabled devices from pairing with the MX7 Tecton while AppLock is in control.

Bluetooth Bar Code Reader Setup

Refer to the Bluetooth scanner manufacturer's User Guide; it may be available on the manufacturer's web site. Contact Technical Assistance (page 16-1) for Bluetooth product help.

Introduction

Honeywell supports several different types of bar code readers. This section describes the interaction and setup for a mobile Bluetooth laser scanner or laser imager connected to the MX7 Tecton using Bluetooth functions.

Prerequisites:

- The MX7 Tecton must have the Bluetooth hardware and software installed. An operating system upgrade may be required. Contact Technical Assistance for details.
- If the MX7 Tecton has a Bluetooth address identifier bar code label affixed, then Bluetooth hardware and software are installed.
- The mobile Bluetooth laser scanner / laser imager battery is fully charged.
- The MX7 Tecton main battery is fully charged. Alternatively, the MX7 Tecton may be cabled to AC/DC power.
- Important: The bar code numbering examples in this segment are not real and should not be created or scanned with a Bluetooth scanner.
- Open the Bluetooth control panel or tap the Bluetooth icon.

Locate the bar code label, similar to the one shown above, attached to the MX7 Tecton. The label is the Bluetooth address identifier for the MX7 Tecton.

The Bluetooth mobile scanner requires this information before discovering, pairing, connecting or disconnecting can occur.

The MX7 Tecton Bluetooth address identifier label should be protected from damage (rips, tears, spills, soiling, erasure, etc.) at all times. It may be required when pairing, connecting, and disconnecting new Bluetooth bar code readers.

MX7 Tecton with Label

If the MX7 Tecton has a Bluetooth address bar code label attached, follow these steps:

1. Scan the Bluetooth address bar code label, attached to the MX7 Tecton, with the Bluetooth mobile scanner.
2. If this is the first time the Bluetooth mobile scanner has scanned the MX7 Tecton Bluetooth label, the devices are paired. See Bluetooth Reader Beep and LED Indications (page 7-12). If the devices do not pair successfully, go to the next step.
3. Open the Bluetooth control panel.
4. Tap Discover. Locate the Bluetooth mobile scanner in the Discovery panel.
5. Double-tap the stylus on the Bluetooth mobile scanner. The right-mouse-click menu appears.
6. Select Pair as Scanner to pair the MX7 Tecton with the Bluetooth mobile scanner.

The devices are paired. The Bluetooth mobile bar code reader responds with a series of beeps and an LED flashes.

Note: After scanning the MX7 Tecton Bluetooth label, if there is no beep and no LED flash from the Bluetooth mobile device, the devices are currently paired.

MX7 Tecton without Label

If the MX7 Tecton Bluetooth address bar code label does not exist, follow these steps to create a unique Bluetooth address bar code for the MX7 Tecton:

1. First, locate the MX7 Tecton Bluetooth client MAC Address on the EZPair (or LXEZ Pairing) About panel.
2. Next, create a Bluetooth address bar code label for the MX7 Tecton. Free bar code creation software is available for download on the world wide web. Search using the keywords “bar code create”.
3. The format for the bar code label is as follows:
   - Bar code type must be Code 128.
   - FNC3 character followed by string Uppercase L, lowercase n, lowercase k, uppercase B and then the Bluetooth address (12 hex digits, no colons). For example, *LnkB0400fd002031*.
4. Create and print the label.
5. Scan the MX7 Tecton Bluetooth address bar code label with the Bluetooth bar code reader.

The devices are paired. The Bluetooth bar code reader responds with a series of beeps and LED flashes.

Note: After scanning the MX7 Tecton Bluetooth label, if there is no beep and no LED flash from the Bluetooth device, the devices are currently paired.

Bluetooth Reader Beep and LED Indications

Bluetooth Mobile Device Beep Type

Beep Type from Bluetooth Device	Behavior
Acknowledge label	1 beep
Label rejected	2 beeps at low frequency
Transmission error	Beep will sound high-low-high-low
Link successful	Beep will sound low-medium-high
Link unsuccessful	Beep will sound high-low-high-low

Bluetooth Mobile Device LED

LED on Bluetooth Device	Behavior
Yellow LED blinks at 2 Hz	Linking in progress
Off	Disconnected or unlinked
Yellow LED blinks at 50 Hz	Bluetooth transmission in progress
Yellow LED blinks at the same rate as the paging beep (1 Hz)	Paging
Green LED blinks once a second	Disabled indication

Upon startup, if the Bluetooth mobile scanner sounds a long tone, this means the scanner has not passed its automatic Selftest and has entered isolation mode. If the scanner is reset, the sequence is repeated. Contact Technical Assistance (page 16-1) if you need help.

Bluetooth Printer Setup

The Bluetooth managed printer should be as close as possible, in direct line of sight, with the MX7 Tecton during the pairing process.

1. Open the Bluetooth control panel on the MX7 Tecton.
2. Tap Discover. Locate the Bluetooth printer in the Discovery panel.
3. Tap and hold the stylus (or double-tap) on the Bluetooth printer until the right-mouse-click menu appears.
4. Select Pair as Printer to pair the MX7 Tecton with the Bluetooth managed printer.

The devices are paired. The Bluetooth managed printer may respond with a series of beeps or LED flashes.

Refer to the Bluetooth managed printer manufacturer User's Guide; it may be available on the manufacturer's web site. Contact Technical Assistance (page 16-1) for Bluetooth mobile device help.

Note: If there is no beep or no LED flash from the Bluetooth managed printer, the MX7 Tecton and the printer are currently paired.

8 Data Collection Wedge

Introduction

Set scanner/imager keyboard wedge parameters, enable or disable symbologies from being scanned, scanner icon appearance, active scanner port, and scan key settings. Assign baud rate, parity, stop bits and data bits for available COM ports. Scanner parameters apply to the MX7 Tecton integrated scanner/imager only. Bar code manipulation parameters apply to bar codes scanned by the MX7 Tecton integrated scanner/imager engine.

Scanner configuration can be changed using the Data Collection settings panels or via the API functions. While the changed configuration is being read, the Scanner LED is solid amber. The scanner is not operational during the configuration update.

The MX7 Tecton has one integrated bar code scanner/imager port. Only one scan engine is installed at a time. Scan engines are not “hot swappable”. The MX7 Tecton may have one of the following integrated bar code decoding engines:

- Short Range Laser Scanner, 955I
- Base Laser Scanner, 955E
- Multi-Range “LORAX” Laser, 1524ER
- Hand Held Products 2D Area Imager, 5300
- Honeywell Laser Scanner, N43XX
- Honeywell Laser Scanner, N73XX

Note: Identify the Scan Engine: Open the Data Collection application panel on the MX7 Tecton. Tap the About tab. The type of integrated scan engine is shown in the Scanner segment.

The integrated scan engine activates when the Scan button on the front of the MX7 Tecton is depressed or when the trigger on an installed trigger handle is depressed.

Symbol or Honeywell scanner

Refer to the *Integrated Scanner Programming Guide* for instruction on configuring specific scanner/imager parameters by using the MX7 Tecton to scan engine-specific setup bar codes in the guide.

Note: Base Laser Scanner, 955E does not support aim mode. Any attempt to adjust the aiming beam using 955E programming bar codes will fail. The Base Laser scanner does not decode Codablock, Code93i or Telepen symbologies.

Hand Held Products Imager

Use the (Hand Held Products) HHP Products button on the Data Options tab and the Advanced button available on many of the individual Symbology Settings screens to configure the Hand Held Products Imager. There are no configuration bar codes for this imager.

Data Processing Overview

Bar code data processing involves several steps. Some steps may be skipped during the processing depending on user selections on the Symbology Settings panels. The steps are presented below in the order they are performed on the scanned data.

1. Scanned data is tested for a code ID and length (Min/Max). If it matches, it is processed per the rules in place for that symbology. If the scan does not meet the criteria for that symbology, it is processed based on the settings for All. If a code ID is not found, the bar code data is processed based on the settings for All.
2. If the symbology is disabled, the scan is rejected.
3. Strip leading data bytes unconditionally.
4. Strip trailing data bytes unconditionally.
5. Parse for, and strip if found, Data Options strings.
6. Replace any control characters with string, as configured.
7. Add prefix string to output buffer.
8. If Code ID is not stripped, add saved code ID from above to output buffer.
9. Add processed data string from above to output buffer.
10. Add suffix string to output buffer.
11. Add a terminating NUL to the output buffer, in case the data is processed as a string.
12. If key output is enabled, start the process to output keys. If control characters are encountered:
    - If Translate All is set, key is translated to CTRL + char, and output.
    - If Translate All is not set, and key has a valid VK code, key is output.
    - Otherwise, key is ignored (not output).
13. If key output is disabled, a windows message is broadcast to notify listening applications that data is available.

The manipulated data is ready to be read by applications.

Note: When returning scanner or imager to factory default settings: After scanning the scanner-engine-specific bar code to reset all scanner parameters to factory default settings (i.e., Reset All, Set Factory Defaults, Default Settings, etc.), the next step is to open the Data Collection settings panel. Tap OK and close the Data Collection panel. This action will synchronize all scanner formats for your device. Another option you can use to reset the Data Collection panel is to scan the LXEReset bar code (for Symbol and Hand Held Products scan engines) or the Reset bar code (for the N43XX and N73XX Laser Scanners). The LXEReset and Reset bar codes are located in the Integrated Scanner Programming Guide.

Main

The Data Collection Wedge supports up to three concurrent data collection devices. For example, the internal scanner could be used to collect data at the same time a Bluetooth scanner is paired and/or a serial device is attached to COM1. The MX7 Tecton must be in a desktop cradle to use a tethered scanner.

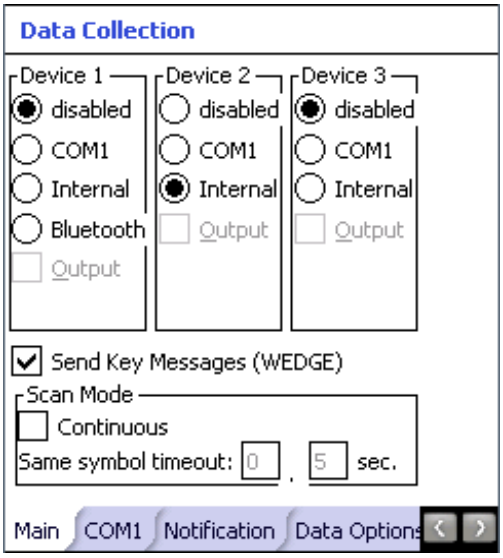
Setting	Default
Device 1	Disabled
Device 2	Internal
Device 3	Disabled
Output	Disabled
Send Key Messages	Enabled
Scan Mode - Continuous	Disabled
Scan Mode - Timeout between same symbol	1 second

Device 1 – Internal. Radio button allows scanner input/output on Device 1 (scan key or trigger).

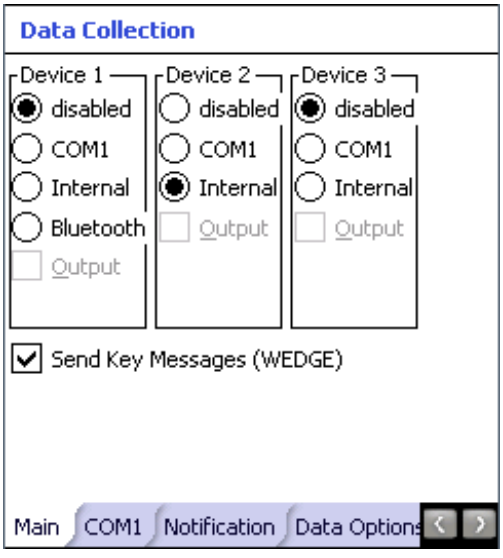
Device 2 – Output is enabled when COM1 is enabled on this port.

Device 3 – Output is enabled when COM1 is enabled on this port.

Note: Since Internal is the default setting for Device 2, a Bluetooth scanner can be paired with the Wedge using EZ Pair (or LXEZ Pairing) on Device 1 without disabling the internal scanner.



Panel showing options for Symbol or Honeywell scan engine



Panel showing options for any other type of scan engine

Output – When Output is enabled, data is received from the scanner and processed via the wedge but an application can also open the WDG0: device and write data to it. An example is when a printer is connected to the same COM port as the scanner via a switch. Data can be written to the WDG device and is redirected to the associated COM port. The application must open the WDG0: port, not the COMx: port as the Wedge has exclusive rights to the COM port. If Output is not enabled, the WDG0: port can still be opened, but any attempts to write to that port fail.

Adjust the settings and tap ok to save the changes. The changes take effect immediately.

Continuous Scan Mode

Note: Do not scan decoder engine configuration bar codes when Continuous scan mode is on. Configuration bar codes do not decode when scanned while Continuous Mode is On.

Continuous scan mode is only available if the MX7 Tecton is equipped with a Symbol or a Honeywell scanner. Continuous scan mode draws power from the main battery every time a scan read/decode sequence is performed.

Enabling Continuous Scan Mode will ensure the laser is always on and decoding.

⚠	Caution: Laser beam is emitted continuously. Do not look or stare into the laser beam.

Set the Timeout between same symbol to a value sufficient to prevent the beeper from continuously beeping when a symbol is left in the scanner's field of view.

If trigger mode, power mode, or timeout between same symbol parameters are changed using external configuration bar codes in the *Integrated Scanner Programming Guide*, the operating system automatically restores the parameters to their programmed settings upon a cold boot and/or any change made in the Data Collection settings.

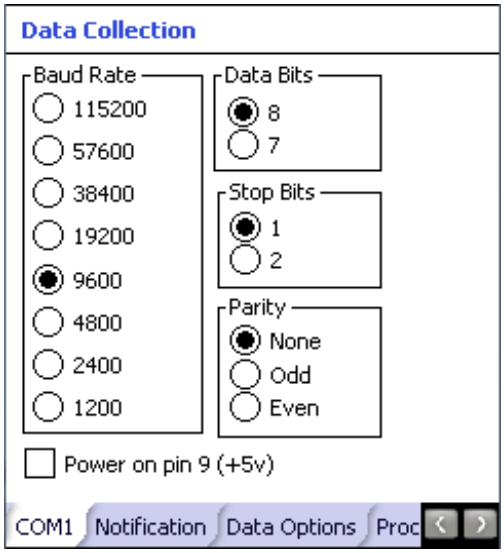
When the scanner is in continuous mode the trigger and scan buttons function as a scanner On/Off switch.

The scanner red LED will always be off in continuous mode. The audio beeps and green LED function the same as they do for normal trigger mode.

Switching to and from continuous and normal trigger modes is in effect after upon tapping the ok button and waiting for the amber scan LED to go out. A reboot is not required or necessary.

COM1

Setting	Default
Baud Rate	9600
Data Bits	8
Stop Bits	1
Parity	None



Integrated laser scanner default values are 9600 Baud, 8 data bits, 1 stop bit and No parity.

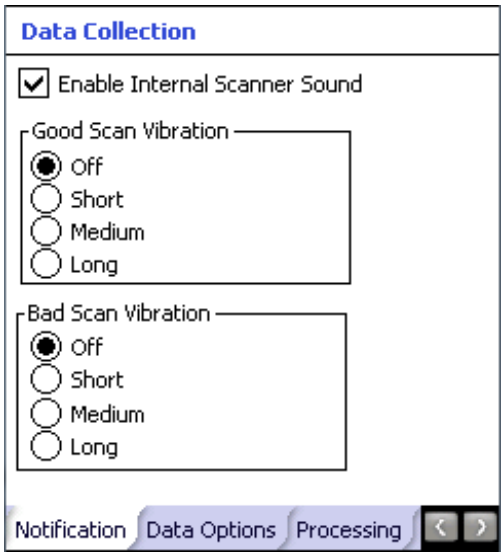
If these values are changed, the default values are restored after a cold boot or after re-imaging the OS.

COM1 does not support 5V switchable power on Pin 9 for tethered scanners.

Notification

Use this panel to toggle internal scanner sounds on and off. Internal scanner sound, by default, is enabled.

Setting	Default
Enable Internal Scanner Sound	Enabled
Good Scan Vibration	Off
Bad Scan Vibration	Off



Vibration

Enable Good scan vibration or Bad scan vibration when a tactile response on a good scan or bad scan is desired. Scan sounds are accompanied by a tactile response when the internal scanner Sound parameter is enabled.

Enable short, medium or long duration for each selection (good scan and bad scan).

Adjust the settings and tap ok to save the changes. The changes take effect immediately.

Since the Data Collection Wedge uses the operating system interface to emit sounds/beeps, if the volume/vibrate icon is set to anything other than On, Wedge beeps do not sound. Wedge vibration is not affected by the System setting.

Beep/sound volume and vibration can be quickly toggled on and off by tapping the volume icon on the Windows Mobile Today screen.

Data Options

Bar code manipulation parameter settings on this tab are applied to the incoming data resulting from successful bar code scans sent to the MX7 Tecton for processing.

Note: The Data Options tab contains only those options available for one type of decoding engine.

Setting	Default
Enable Code ID	None
Symbology Settings	All
Control Character Translate All	Disabled
Custom IDs	Name blank
HHP Properties (Hand Held Products)	Options Disabled: Centering DecodeMode LinearRange AimTimer LeaveLightsOn

The Data Options tab contains several options to control bar code processing. Options include:

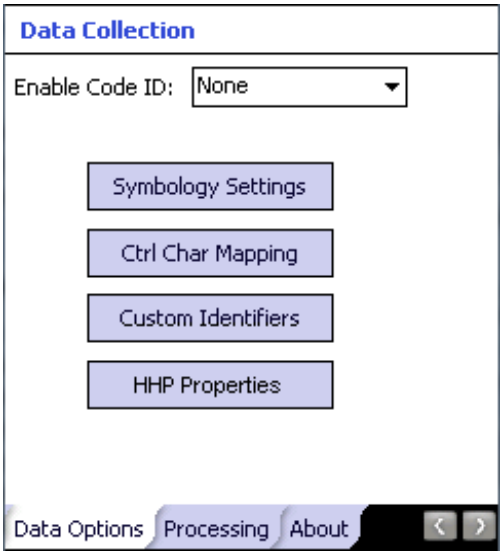
- Defining custom Code IDs
- Disable processing of specified bar code symbologies
- Rejecting bar code data that is too short or too long
- Stripping characters including Code ID, leading or trailing characters and specified bar code data strings
- Replacing control characters
- Adding a prefix and a suffix

For MX7 Tecton with Symbol or Honeywell engine:

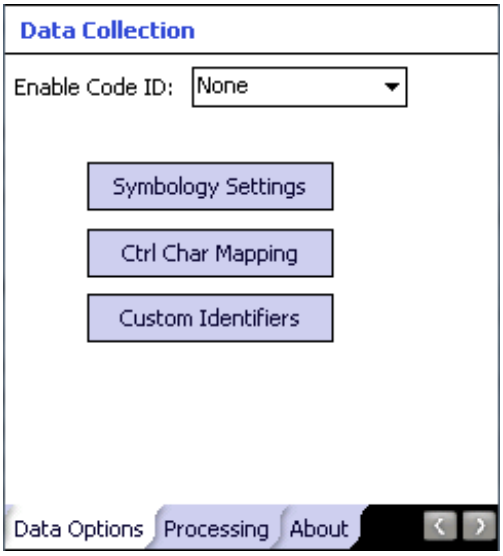
Data Collection Wedge can only enable or disable the processing of a bar code inside the Wedge software. Enabling or disabling a specific bar code symbology at the scanner/imager is done manually using the configuration bar codes in the *Integrated Scanner Programming Guide*.

For MX7 Tecton with Hand Held Products Imager:

Data Collection Wedge enables or disables the bar code at the imager as well as enabling or disabling the bar code processing in the Wedge software..



Panel for a Hand Held Products scan engine



Panel for any other type of scan engine

The HHP Properties button is only present if the MX7 Tecton is equipped with a Hand Held Products (HHP) imager.

1. Choose an option in the Enable Code ID drop-down box:
   - None
   - AIM
   - Honeywell
   - Symbol
   - HHP
   - Custom.
2. The Symbology screen is displayed.

Enable Code ID

This parameter programs the internal scanner to transmit the specified Code ID and/or determines the type of bar code identifier being processed. If the scanner being configured is not an integrated scanner, the scanner driver expects that the setting has been programmed into the scanner externally, and that the data will be coming in with the specified Code ID attached.

Transmission of the Code ID is enabled at the scanner for all bar code symbologies, not for an individual symbology. Code ID is sent from the scanner so the scanner driver can discriminate between symbologies.

- When Strip: Code ID (see Symbology panel) is not enabled, the code ID is sent as part of the bar code data to an application.
- When Strip: Code ID (see Symbology panel) is enabled, the entire Code ID string is stripped (i.e., treated as a Code ID).
- UPC/EAN Codes only: The Code ID for supplemental bar codes is not stripped.
- When Enable Code ID is set to AIM, Symbol or HHP, Custom Code IDs appear at the end of the list of standard Code IDs.
- When Enable Code ID is set to Custom, Custom Code IDs replace the list of standard Code IDs.
- Symbol equipped devices are configured using configuration bar codes, When Enable Code ID is set to Custom, AIM or Symbol Code IDs must be added to the end of the Custom Code ID. For example, if a Custom Code ID ‘AAA’ is created to be read in combination with an AIM ID for Code 39 ‘]A1’, the Custom Code ID must be entered with the AIM ID code first then the Custom Code ID :]A1AAA.
- When Enable Code ID is set to None, Code IDs are ignored.
- Custom symbologies appear at the end of the list in the Symbology dialog, but will be processed at the beginning of the list in the scanner driver. This allows custom IDs, based on actual code IDs, to be processed before the Code ID.
- The external scanner operation cannot be controlled by the MX7 Tecton scanner driver; therefore, a ‘good’ beep may be sounded from the external scanner even if a bar code from an external scanner is rejected because of the configuration specified. The MX7 Tecton will still generate a ‘bad’ scan beep, to indicate the bar code has been rejected.

Enable Code ID Options

Depending on the model of the scanner installed, some combination of the following IDs are listed.

None

Programs the internal scanner to disable transmission of a Code ID. The only entry in the Symbology popup list is All.

AIM

Programs the internal scanner to transmit the AIM ID with each bar code. The combo box in the Symbology panel is loaded with the known AIM ID symbologies for that platform, plus any configured Custom code IDs.

Honeywell

Programs the internal scanner to transmit the Honeywell ID with each bar code. The combo box in the Symbology panel is populated with the known Honeywell ID symbologies for that platform, plus any configured Custom code IDs.

Symbol

Programs the internal scanner to transmit the Symbol ID with each bar code. The combo box in the Symbology panel is loaded with the known Symbol ID symbologies for that platform, plus any configured Custom Code IDs.

HHP (Hand Held Products)

The imager always transmits the HHP ID with each bar code, so the Code ID is used to identify the bar code being processed. The combo box in the Symbology control panel is populated with the known HHP ID symbologies for that platform, plus any configured Custom code IDs.

Custom

Does not change the scanner's Code ID transmission setting. The combo box in the Symbology panel is loaded with any configured Custom Code IDs.

Enable Code ID Buttons

Symbology Settings

Individually enable or disable a bar code from being scanned, set the minimum and maximum size bar code to accept, strip Code ID, strip data from the beginning or end of a bar code, or (based on configurable Barcode Data) add a prefix or suffix to a bar code before transmission.

Ctrl Char Mapping

Define the operations the Wedge performs on control characters (values less than 0x20) embedded in bar codes.

Custom Identifiers

Defines an identifier that is at the beginning of bar code data which acts as a Code ID. After a Custom Identifier is defined, Symbology Settings can be defined for the identifier just like standard Code IDs.

HHP Properties

Set properties for a Hand Held Products imager including centering, mode, range, AIM timer and light behavior. Note that the HHP Properties button is only present if the MX7 Tecton is equipped with a Hand Held Products imager.

Symbology Settings

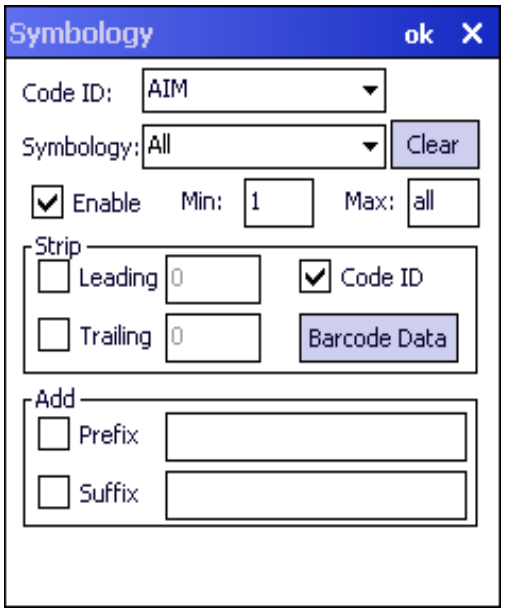
The Symbology selected in the Symbology drop down list defines the symbology for which the data is being configured. The features available on the Symbology panel include the ability to:

- individually enable or disable a bar code from scanning,
- set the minimum and maximum size bar code to accept,
- strip Code ID,
- strip data from the beginning or end of a bar code,
- or (based on configurable Barcode Data) add a prefix or suffix to a bar code.

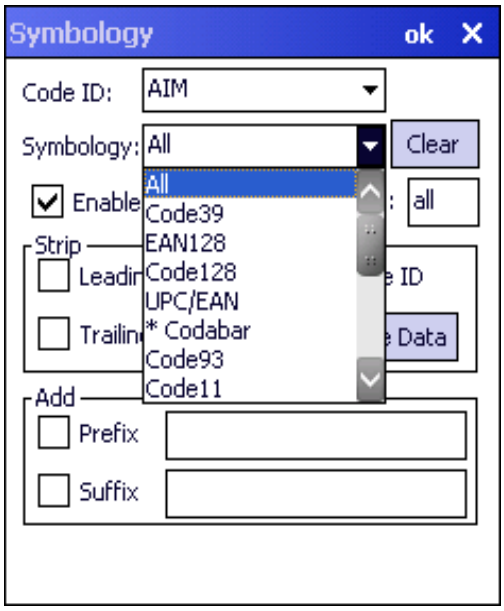
The Code ID drop down box only filters the available symbologies in the Symbology drop down box by the selected Code ID. This Code ID box does not enable or disable the Code ID as that function is controlled by the Enable Code ID box on the Data Options tab.

The Symbology drop down box contains all symbologies supported based on the Code ID selected above. An asterisk appears in front of symbologies that have already been configured or have been modified from the default value.

Each time a Symbology is changed, the settings are saved as soon as the ok button is clicked. Settings are also saved when a new Symbology is selected from the Symbology drop down list.



Panel for HHP scan engine



Panel for Honeywell scan engine

Clear Button

This button will erase any programmed overrides, returning to the default settings for the selected symbology.

If Clear is pressed when All is selected as the symbology, a confirmation dialog appears. Tap the Yes button and all symbologies are reset to their factory defaults, and all star (*) indications are removed from the list of Symbologies.

Advanced Button

If there are advanced configuration options for the selected symbology, an Advanced button is displayed in the lower right corner of the panel. Not all bar code symbologies have configuration parameters so the Advanced button is not present for all symbologies.

Because the Hand Held Products imager does not support configuration bar codes, the Advanced button function allows configuration parameters to be set for many of the supported bar codes.

Processing Order

The order in which these settings are processed are:

- Min / Max
- Code ID
- Leading / Trailing
- Barcode Data
- Prefix / Suffix

Note: When Enable Code ID is set to None on the Data Options tab and All is selected in the Symbology field, Enable and Strip Code ID on the Symbology panel are dimmed and the user is not allowed to change them, to prevent deactivating the scanner completely.

When All is selected in the Symbology field and the settings are changed, the settings in this dialog become the defaults, used unless overwritten by the settings for individual symbologies. This is also true for Custom IDs, where the code IDs to be stripped are specified by the user.

Note: In Custom mode on the Data Options tab, any Code IDs not specified by the user will not be stripped, because they will not be recognized as Code IDs.

If a specific symbology's settings have been configured, a star (*) will appear next to it in the Symbology drop down box, so the user can tell which symbologies have been modified from their defaults.

If a particular symbology has been configured, the entire set of parameters from that symbologies screen are in effect for that symbology. In other words, either the settings for the configured symbology will be used, or the default settings are used, not a combination of the two.

If a symbology has not been configured (does not have an * next to it) the settings for All are used which is not necessarily the default.

Enable, Min, Max

Enable

This check box enables (checked) or disables (unchecked) the symbology field.

The scanner driver searches the beginning of the bar code data for the type of ID specified in the Data Options tab -- Enable Code ID field plus any custom identifiers.

When a code ID match is found as the scanner driver processes incoming bar code data, if the symbology is disabled, the bar code is rejected. Otherwise, the other settings in the dialog are applied and the bar code is processed.

If the symbology is disabled, all other fields on this dialog are dimmed.

If there are customized settings, uncheck the Enable check box for the All symbology. This results in disabling all symbologies except the customized ones.

Min

This field specifies the minimum length that the bar code data (not including Code ID) must meet to be processed.

Any bar code scanned that is less than the number of characters specified in the Min field is rejected. The default for this field is 1.

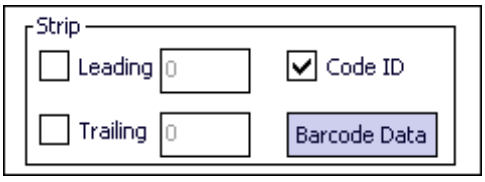
Max

This field specifies the maximum length that the bar code data (not including Code ID) can be processed. Any bar code scanned that has more characters than specified in the Max field is rejected. The default for this field is All (9999).

If the value entered is greater than the maximum value allowed for that symbology, the maximum valid length is used instead.

Strip Leading/Trailing Control

This group of controls determines what data is removed from the collected data before the data is buffered for the application. When all values are set, Code ID takes precedence over Leading and Trailing; Barcode Data stripping is performed last. Stripping occurs before the Prefix and Suffix are added, so does not affect them.



If the total number of characters being stripped is greater than the number of characters in the collected data, it becomes a zero byte data string.

If, in addition, Strip Code ID is enabled, and no prefix or suffix is configured, the processing will return a zero-byte data packet, which will be rejected.

The operation of each type of stripping is defined below:

Leading

This strips the number of characters specified from the beginning of the collected data (not including Code ID). The data is stripped unconditionally. This action is disabled by default.

Trailing

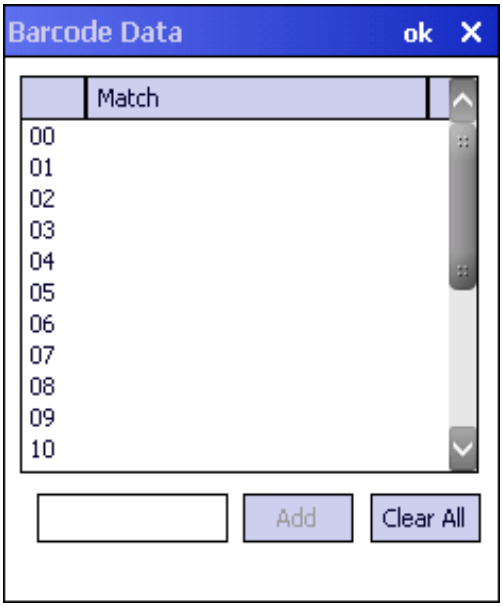
This strips the number of characters specified from the end of the collected data (not including Code ID). The data is stripped unconditionally. This action is disabled by default.

Code ID

Strips the Code ID based on the type code ID specified in the Enable Code ID field in the Data Options tab. By default, Code ID stripping is enabled for every symbology (meaning code IDs will be stripped, unless specifically configured otherwise).

Bar Code Data Match List

The Barcode Data Panel is used to strip data that matches the entry in the Match list from the bar code. Enter the data to be stripped in the text box and tap the Insert or Add button. The entry is added to the Match list.



To remove an entry from the Match list, highlight the entry in the list and tap the Remove button.

Tap ok to store any additions, deletions or changes.

Bar Code Data Match Edit Buttons

Add

Entering data into the text entry box enables the Add button. Tap the Add button and the data is added to the next empty location in the Custom ID list.

Insert

Tap on an empty line in the Custom ID list. The Add button changes to Insert. Enter data into both the Name and ID Code fields and tap the Insert button. The data is added to the selected line in the Custom IDs list.

Edit

Double tap on the item to edit. Its values are copied to the text boxes for editing. The Add button changes to Replace. When Replace is tapped, the values for the current item in the list are updated.

Clear All

When no item in the Custom IDs list is selected, tapping the Clear All button clears the Custom ID list and any text written (and not yet added or inserted) in the Name and ID Code text boxes.

Remove

The Clear All button changes to a Remove button when an item in the Custom IDs list is selected. Tap the desired line item and then tap the Remove button to delete it. Line items are Removed one at a time. Contents of the text box fields are cleared at the same time.

Notes

- Prefix and Suffix data is always added on after stripping is complete, and is not affected by any stripping settings.
- If the stripping configuration results in a 0 length bar code, a good beep will still be emitted, since bar code data was read from the scanner.

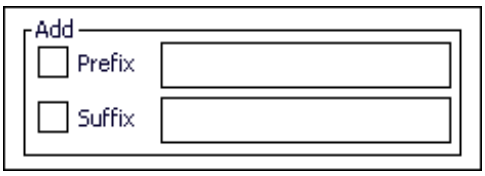
Match List Rules

The data in the match list is processed by the rules listed below:

- Strings in the list will be searched in the order they appear in the list. If the list contains ABC and AB, in that order, incoming data with ABC will match first, and the AB will have no effect.
- When a match between the first characters of the bar code and a string from the list is found, that string is stripped from the bar code data.
- Processing the list terminates when a match is found or when the end of the list is reached.
- If the wildcard * is not specified, the string is assumed to strip from the beginning of the bar code data. The string ABC* strips off the prefix ABC. The string *XYZ will strip off the suffix XYZ. The string ABC*XYZ will strip both prefix and suffix together. More than one * in a configuration string is not allowed. (The User Interface will not prevent it, but results would not be as expected, as only the first * is used in parsing to match the string.)
- The question mark wildcard ? may be used to match any single character in the incoming data. For example, the data AB?D will match ABCD, ABcD, or AB0D, but not ABDE.
- The data collected is saved per symbology configured. The Symbology selected in the Symbologies dialog defines the symbology for which the data is being configured.
- Note that the Code ID (if any are configured) is ignored by this dialog, regardless of the setting of Strip: Code ID in the Symbologies dialog. According to the sequence of events (specified above), the Code ID must not be included in the bar code data being matched, because when the matching test occurs, the Code ID has already been stripped. If Strip Code ID is disabled, then the bar code data to match must include the Code ID. If Strip Code ID is enabled, the data should not include the Code ID since it has already been stripped.

Add Prefix/Suffix Control

Note: Non-ASCII equivalent keys in Key Message mode are unavailable in this option. Non-ASCII equivalent keys include the function keys (e.g., <F1>), arrow keys, Page up, Page down, Home, and End.



Use this option to specify a string of text, hex values or hat encoded values to be added to the beginning (prefix) or the end (suffix) of the bar code data. Up to 19 characters can be included in the string. The string can include any character from the keyboard plus characters specified by hex equivalent or entering in hat encoding. See Hat Encoding (page 8-39) for a list of characters with their hex and hat-encoded values.

Using the Escape function allows entering literal hex and hat values.

Add Prefix

To enable a prefix, check the Prefix check box and enter the desired string in the textbox. The default is disabled (unchecked) with a blank text string.

When bar code data is processed, the Prefix string is sent to the output buffer before any other data. Because all stripping operations have already occurred, stripping settings do not affect the prefix.

The prefix is added to the output buffer for the Symbology selected from the pulldown list. If ‘All’ is selected, the prefix is added for any symbology that has not been specifically configured.

Add Suffix

To enable a suffix, check the Suffix check box and enter the desired string in the textbox. The default is disabled (unchecked) with a blank text string.

When bar code data is processed, the Suffix string is sent to the output buffer after the bar code data. Because all stripping operations have already occurred, stripping settings do not affect the suffix.

The suffix is added to the output buffer for the Symbology selected from the pulldown list. If ‘All’ is selected, the suffix is added for any symbology that has not been specifically configured.

Symbologies

The Code ID drop-down box filters the available symbologies, in the Symbology drop down box, by the selected Code ID.

When a Honeywell scan engine is installed, AIM, Custom and Honeywell symbologies are displayed.

When a Hand Held Products imager scan engine is installed, AIM, Custom and HHP symbologies are displayed. HHP does not support Symbol IDs.

When a Symbol scan engine is installed, AIM, Custom and Symbol symbologies are displayed. Symbol does not support HHP IDs (Hand Held Products) or Honeywell IDs.

AIM Symbologies

Note: When the integrated scan engine is a Honeywell or Symbol scan engine, AIM IDs apply, but Advanced properties do not and the Advanced button is not available.

Symbol Engine	Honeywell Engine
All	All
Aztec	Codabar
Codabar	Code 11
Code 128	Code 128
Code 39	Code 39
UPC/EAN	Code 93
Code 49	EAN/UPC
Code 93	GS1 Databar
Data Matrix	Interleaved 2 of 5
Interleaved 2 of 5	Matrix 2 of 5
MaxiCode	MSI
MicroPDF	NEC 2 of 5
PDF417	Plessey
PosiCode	Str2of5
QR Code	Telepen
GS1 DataBar	Trioptic Code
	China Post

The Data Collection Wedge does not manage mutually exclusive option selections. The user is responsible for understanding the options that can co-exist for the data collection device. The documentation provided from the manufacturer of the scanner/imager being managed describes the interaction between symbologies and their configurations.

HHP Symbologies

Advanced properties are available when an integrated Hand Held Products imager is installed in the MX7 Tecton. Advanced properties are applicable regardless of the ID type selected (AIM or HHP). HHP = Hand Held Products.

Not all HHP symbologies have Advanced options. Symbologies with Advanced options are documented on the following pages. Symbologies with Advanced button function are marked with an asterisk in the table below.

Symbology				
All	Composite	ISBT-1	RSS	AUSPOST
Aztec	Coupon	Matrix 2 of 5	Strt25	JapanPost
BPO	DataMatrix	Mesa *	Strt32	Planet *
Codabar *	EAN *	MSI *	Telepen *	DutchPost
Codablock	EAN13 *	Other	TLC	ChinaPost
Code 11 *	EAN128	PDF417	Trioptic39	Code16K
Code32	GenCode128	Plessey	UPCA *	Usps4cb
Code 39 *	IATA25	Posicode *	UPCE0 *	Maxicode
Code 49	IDTag	Postnet	UPCE1 *	MicroPDF
Code 93	Interleaved 2 of 5 *	QR	CANPOST	OCR *
Code 128				

The Data Collection Wedge does not manage mutually exclusive option selections. The user is responsible for understanding the options that can co-exist for the data collection device. The documentation provided from the manufacturer of the scanner/imager being managed describes the interaction between symbologies and their configurations.

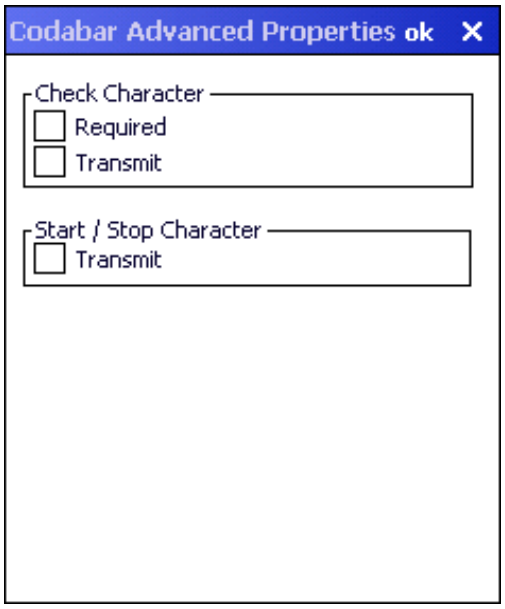
Advanced Button (Hand Held Products Imager Only)

The Advanced button is only available if a Hand Held Products Imager is in use. Because the Hand Held Products imager does not support configuration bar codes (available in the *Integrated Scanner Programming Guide*), the Advanced button function allows configuration parameters to be set for many of the HHP imager supported bar codes.

If there are advanced configuration options for the selected Hand Held Products Imager symbology, an Advanced button is displayed in the lower right corner of the panel. When the Enable check box is empty, the Advanced button is dimmed for a symbology with advanced configuration parameters. Not all bar code symbologies have configuration parameters so the Advanced button is not present for all symbologies.

Sections that follow are the HHP symbologies with advanced configuration parameters that can be changed by the user.

Codabar - Advanced Properties



Check Character

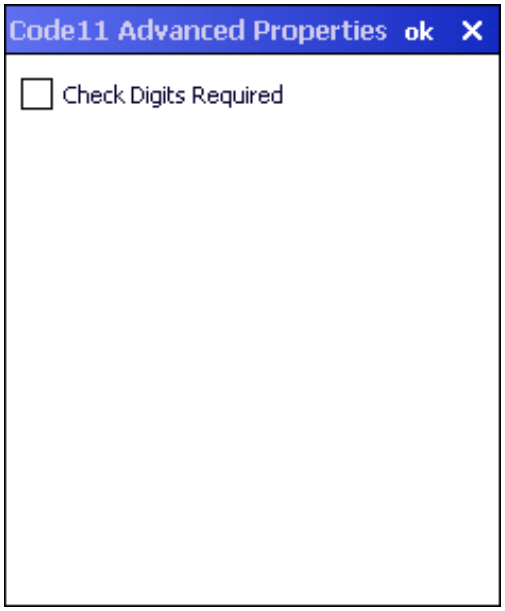
Required – When enabled, the check character is required. Default is disabled.

Transmit – When enabled, the check character is transmitted. Default is disabled.

Start / Stop Character

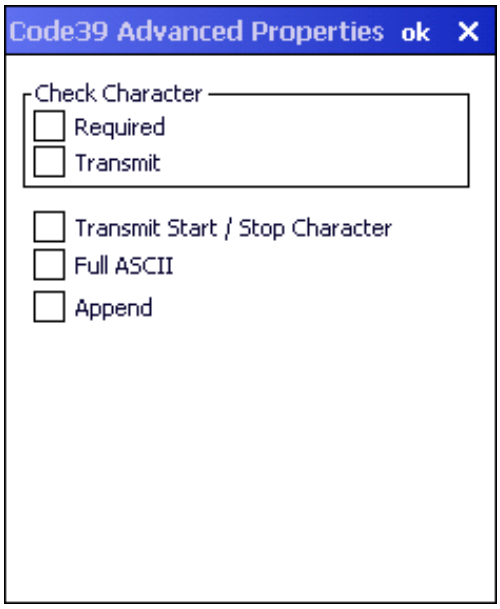
Transmit – When enabled, the start / stop characters are transmitted. Default is disabled.

Code11 - Advanced Properties



Check Digits Required – When enabled, only bar codes with two check digits are decoded. The default is disabled.

Code39 - Advanced Properties



Check Character

Required – When enabled, the check character is required. Default is disabled.

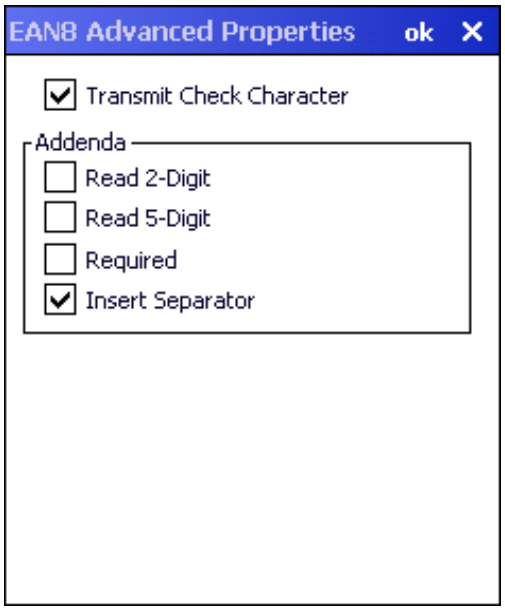
Transmit – When enabled, the check character is transmitted. Default is disabled.

Transmit Start / Stop Character – When enabled, the start / stop characters are transmitted. Default is disabled.

Full ASCII – When enabled, full ASCII interpretation is used. Default is disabled.

Append – When enabled, append and buffer codes that start with a space. Default is disabled.

EAN8 - Advanced Properties



Transmit Check Character – When enabled, transmit the check character. Default is enabled.

Addenda

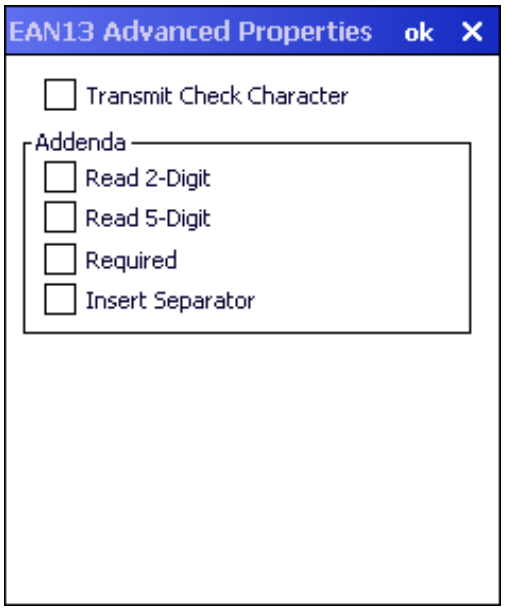
Read 2-Digit – When enabled, transmit the 2 digit addenda. Default is disabled.

Read 5-Digit – When enable, transmit the 5 digit addenda. Default is disabled.

Required – When enabled, only transmit bar codes with a 2 or 5 digit addenda. Default is disabled.

Insert Separator – When enabled, insert a space between the code and addenda. Default is enabled.

EAN13 - Advanced Properties



Transmit Check Character – When enabled, transmit the check character. Default is disabled.

Addenda

Read 2-Digit – When enabled, transmit the 2 digit addenda. Default is disabled.

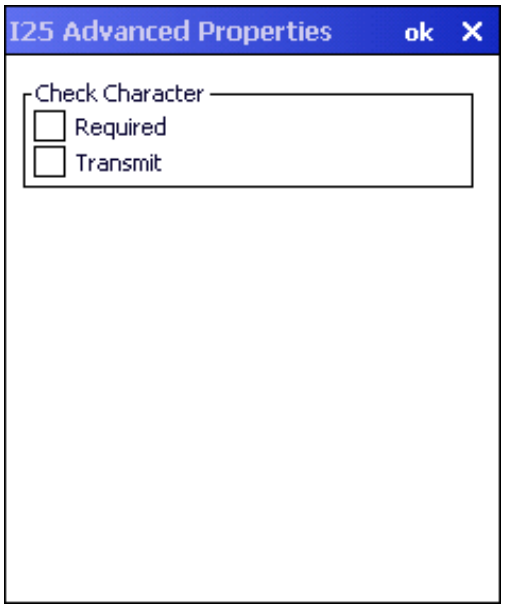
Read 5-Digit – When enable, transmit the 5 digit addenda. Default is disabled.

Required – When enabled, only transmit bar codes with a 2 or 5 digit addenda. Default is disabled.

Insert Separator – When enabled, insert a space between the code and addenda. Default is disabled.

Note: A UPCA decoding algorithm will also decode EAN 13 labels. For correct operation, either disable the UPCA symbology when using EAN 13 labels or configure the UPCA settings to match the EAN 13 settings.

Interleaved 2 of 5 - Advanced Properties

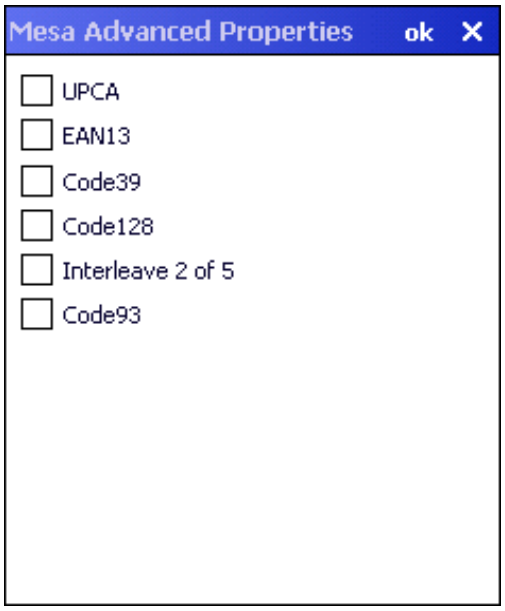


Check Character

Required – When enabled, the check character is required. Default is disabled.

Transmit – When enabled, the check character is transmitted. Default is disabled.

Mesa - Advanced Properties



UPCA – When enabled, decode UPCA Mesa. Default is disabled.

EAN13 – When enabled, decode EAN 13 Mesa. Default is disabled.

Code39 – When enabled, decode Code 39 Mesa. Default is disabled.

Code128 – When enabled, decode Code 128 Mesa. Default is disabled.

Interleaved 2 of 5 – When enabled, decode Interleaved 2 of 5 Mesa. Default is disabled.

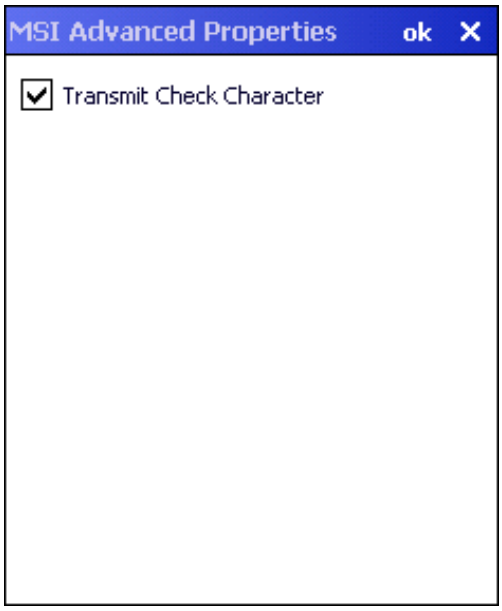
Code93 – When enabled, decode Code 93 Mesa. Default is disabled.

When the Mesa symbology is chosen on the Symbology panel (the Enable check box is checked) the Advanced button must be clicked and the desired Mesa Advanced Properties sub-symbology selected.

When Mesa is disabled on the Symbology panel (the Enable check box is cleared), tap the Advanced button and uncheck all parameters or sub-symbologies, on the Mesa Advanced Properties panel.

Note: The root symbology (UPCA, EAN13, Code39, Code128, Interleaved 2 of 5 and/or Code 93) must be enabled before the matching enabled Mesa sub-symbology will decode.

MSI - Advanced Properties



Transmit Check Character – When enabled, transmit the check character. Default is enabled.

OCR Properties - Advanced

Font – Font selection. Default is disabled.

- A = OCR A
- B = OCR B
- Money = OCR Money
- MICR = Magnetic Ink Character Recognition

Direction – Decoder reads OCR fonts in any direction, but setting direction parameter correctly can increase decoding speed. Default is Left to Right.

Template – Template length must match the length of OCR string to be read. Default is dddddddd. Valid template selections are:

- a - alphanumeric character (digit or letter)
- c - check character
- d - digits from 0 to 9
- e - any character
- g - any character specified in group G
- h - any character specified in group H
- l - alphabetic letter
- r - delimits a row
- t - delimits multiple templates

All characters are transmitted as is except for the selected template.

Group G – Null terminated string defines the set of characters in group G. The default is null.

Group H – Null terminated string defines the set of characters in group H. The default is null.

Check – Enter the string constant 0123456789 for modulo10 checksums and the string constant 0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ for modulo36 checksums.
The default is null.

OCR Template Examples

1. To read a combination of 6 alpha and numeric characters use the following template:

```
aaaaaa
```

2. To read the same string with a modulo 10 check digit in the seventh character position, use the following template:

   ```
   aaaaaac
   ```

   Then enter 0123456789 for the Check parameter.

3. To read either a string of 6 alphabetic letters OR a string of 8 numeric digits, use this template:

   ```
   lllllltddddddd
   ```

   Note the use of the “t” to separate the first template from the second.

4. To read multiple rows of OCR data as shown below:

   ```
   123456
   ABCDEF
   ```

   Either of the following templates could be used:

   ```
   ddddddrllllll  or  aaaaaaraaaaaa
   ```

   Note the use of the “r” to define the position of the second row.

OCR Checksum Calculation

The following explains how the checksum is generated for the OCR bar code:

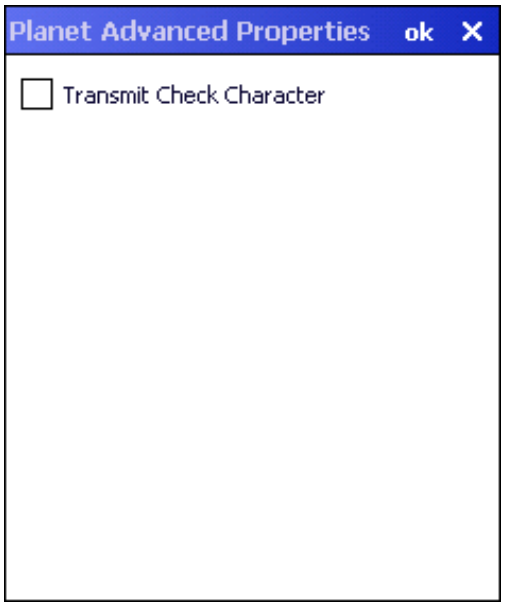
Modulo 10:

1. Add the characters in the string (not including the checksum character). Valid values are 0 – 9 for modulo 10.
2. Subtract 10 from the sum obtained above. Continue subtracting 10 until the remainder is less than 10.
3. The remainder obtained above is the checksum. Enter this digit in the checksum position.

Modulo 36:

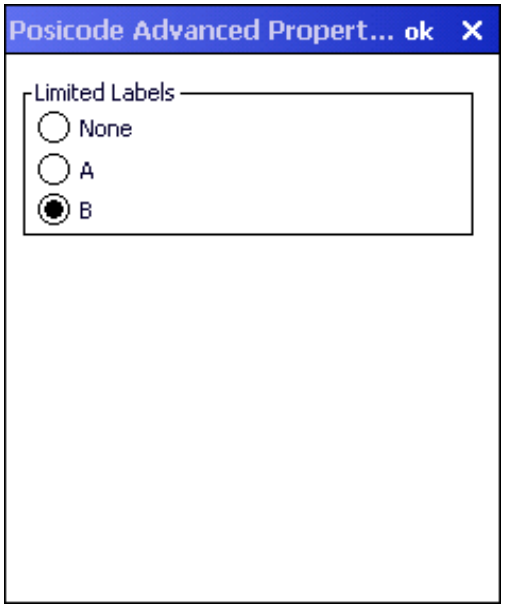
1. Add the characters in the string (not including the checksum character). Digit / Alpha values are defined as follows for modulo 36: 0 – 9 = 0 – 9; A = 10, B = 11, … Z = 25
2. Subtract 36 from the sum obtained above. Continue subtracting 36 until the remainder is less than 36.
3. Subtract the remainder obtained above from 36. The value obtained is the checksum. Enter this character in the checksum position.

Planet - Advanced Properties



Transmit Check Character – When enabled, transmit the check character. Default is enabled.

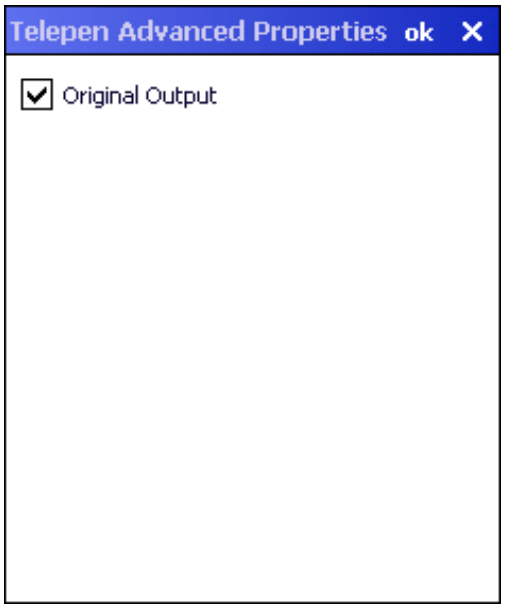
Posicode - Advanced Properties



Limited Labels – Select the type of Posicode Limited labels:

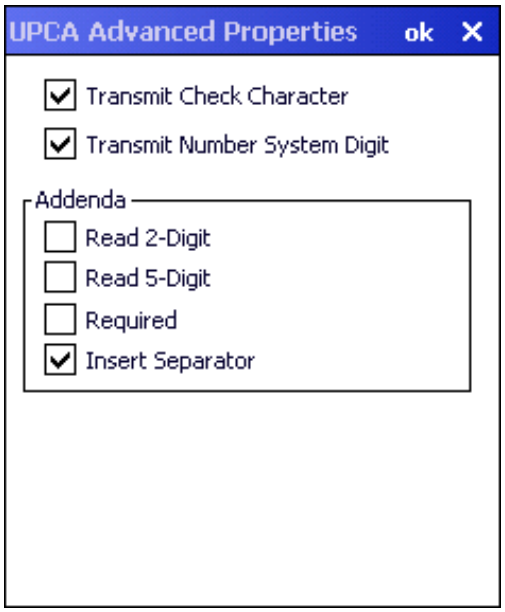
- None
- A – Posicode Limited A
- B – Posicode Limited B

Telepen - Advanced Properties



Original Output – When enabled, output is Original Telepen. When disabled, output is AIM. Default is enabled.

UPCA- Advanced Properties



Transmit Check Character – When enabled, transmit the check character. Default is enabled

Transmit Number System Digit – When enabled, transmit the number system digit. Default is enabled.

Addenda

Read 2-Digit – When enabled, transmit the 2 digit addenda. Default is disabled.

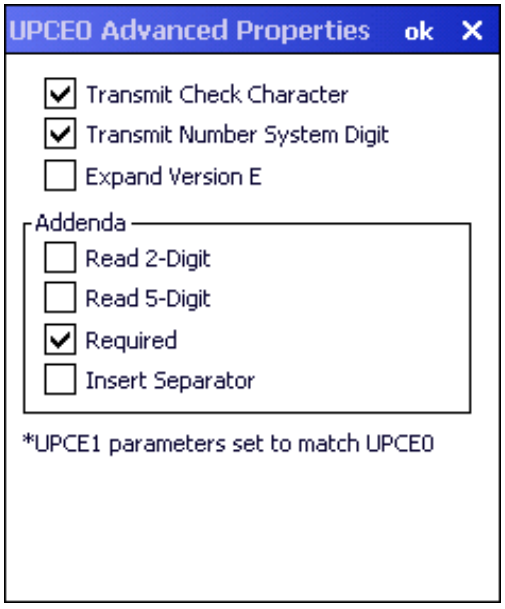
Read 5-Digit – When enable, transmit the 5 digit addenda. Default is disabled.

Required – When enabled, only transmit bar codes with a 2 or 5 digit addenda. Default is disabled.

Insert Separator – When enabled, insert a space between the code and addenda. Default is enabled.

Note: An EAN 13 decoding algorithm will also decode UPCA labels. For correct operation, either disable the EAN 13 symbology when using UPCA labels or configure the EAN 13 settings to match the UPCA settings.

UPCE0- Advanced Properties



Note: The UPCE0 and UPCE1 parameters are always set to match each other. Therefore if a change is made to a parameter to either the EPCE0 or UPCE1 Advanced Properties that same change is automatically made to the Advanced Properties for the other symbology.

Note: UPCE0 and UPCE1 are enabled as the same symbology at the scanner. Therefore, the only way for UPCE1 configuration to be used is if UPCE0 is disabled. When UPCE0 is disabled, it is scanned by the imager but rejected by Data Collection Wedge.

Transmit Check Character – When enabled, transmit the check character. Default is enabled.

Transmit number System Digit – When enabled, transmit the number system digit. Default is enabled.

Expand Version E – When enabled, expand version E to 12-digit UPCA format. Default is disabled.

Addenda

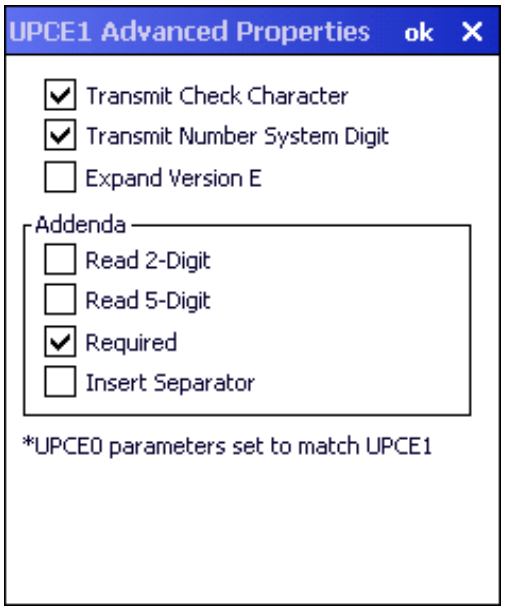
Read 2-Digit – When enabled, transmit the 2 digit addenda. Default is disabled.

Read 5-Digit – When enable, transmit the 5 digit addenda. Default is disabled.

Required – When enabled, only transmit bar codes with a 2 or 5 digit addenda. Default is enabled.

Insert Separator – When enabled, insert a space between the code and addenda. Default is disabled.

UPCE1- Advanced Properties



Note: The UPCE0 and UPCE1 parameters are always set to match each other. Therefore if a change is made to a parameter to either the EPCE0 or UPCE1 Advanced Properties that same change is automatically made to the Advanced Properties for the other symbology.

Note: UPCE0 and UPCE1 are enabled as the same symbology at the scanner. Therefore, the only way for UPCE1 configuration to be used is if UPCE0 is disabled. When UPCE0 is disabled, it is scanned by the imager but rejected by Data Collection Wedge.

Transmit Check Character – When enabled, transmit the check character. Default is enabled

Transmit number System Digit – When enabled, transmit the number system digit. Default is enabled.

Expand Version E – When enabled, expand version E to 12-digit UPCA format. Default is disabled.

Addenda

Read 2-Digit – When enabled, transmit the 2 digit addenda. Default is disabled.

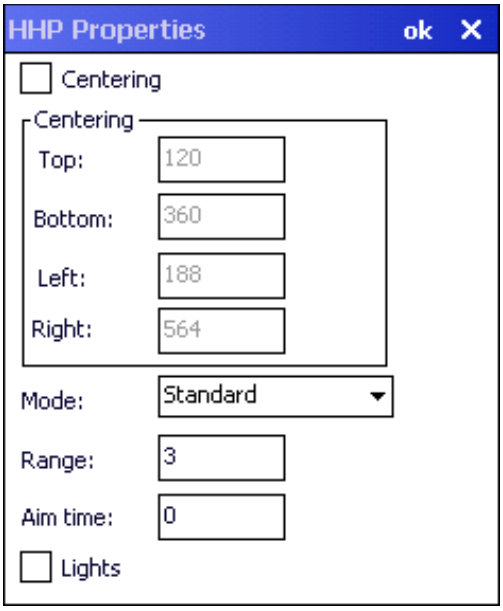
Read 5-Digit – When enable, transmit the 5 digit addenda. Default is disabled.

Required – When enabled, only transmit bar codes with a 2 or 5 digit addenda. Default is enabled.

Insert Separator – When enabled, insert a space between the code and addenda. Default is disabled.

HHP Properties

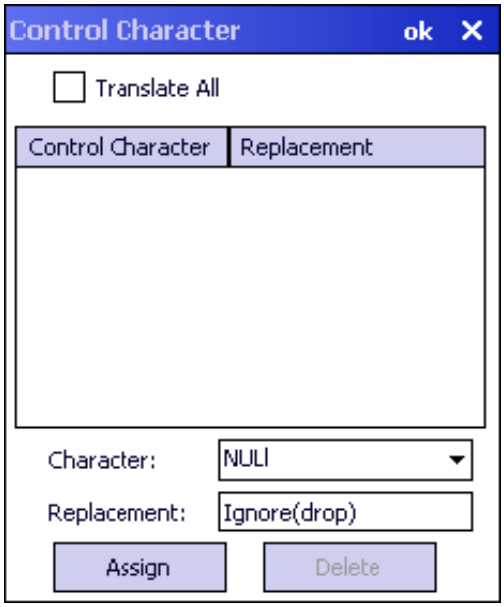
When the MX7 Tecton is equipped with a Hand Held Products imager, this option is used to configure imager scanning parameters.



Option	Action
Centering	The centering feature is used to allow the user to accurately scan a selected bar code among a group of bar codes that are located closely together. When centering is turned on, the imager will only decode bar codes that intersect the centering window defined by the user. The centering window must intersect the center of the bar code. The default centering settings define a 60 pixel square area in the center of the imager's field of view. The default is disabled. When enabled, the following parameters may be entered. *Top: Valid:0 – 239, Default:120* *Bottom: Valid:240 – 479, Default:360* *Left: Valid:0 – 319, Default:188* *Right: Valid:320 – 639, Default:564*
Mode	In Standard mode the imager will decode both linear and 2-D symbologies. In Aggressive Linear Decode mode the imager will only read linear symbologies in this mode, but decoding these is faster and more accurate than Standard Mode. In Quick Omni mode the imager searches for a bar code in a reduced field located around the center of the image. Decoding is faster in this mode, but the user must center the aiming line over the bar code to be read. Both linear and 2-D symbologies can be read in this mode. The default is Standard.
Range	Set the linear range. Valid:1 – 6 Default:3 A value of 1 specifies that the linear range that is searched for a readable label is a tight vertical range near the aimer. A value of 6 specifies that the entire height of the image is to be searched.
AIM	Duration of the imager aim beam in 0.1 second increments. Valid:0 – 50 (0 to 5 seconds) Default:0
Lights	Specifies if the imager's lights and aimer should be left on during the entire decode process. The default is disabled. If disabled, the lights are turned on only during image capture, then turned off while the imager attempts to process and decode the bar code. If enabled, the aimer and lights remain turned on during the entire process. In Aggressive Linear Decode mode, set this parameter to enabled to improve the aimer visibility. See “Mode” above.

Ctrl Char Mapping

The Ctrl Char Mapping button on the Data Options tab activates a dialog to define the operations the Data Collection Wedge performs on control characters (values less than 0x20) embedded in bar codes. Control characters can be replaced with user-defined text which can include hat encoded or hex encoded values. In key message mode, control characters can also be translated to their control code equivalent key sequences.



Translate All

When Translate All is checked, unprintable ASCII characters (characters below 20H) in scanned bar codes are assigned to their appropriate CTRL code sequence when the bar codes are sent in Character mode.

The wedge provides a one-to-one mapping of control characters to their equivalent control+character sequence of key-strokes. If control characters are translated, the translation is performed on the bar code data, prefix, and suffix before the keystrokes are simulated.

Translate All

This option is grayed unless the user has Key Message mode (on the Main tab) selected. In Key Message mode, when this option is enabled, control characters embedded in a scanned bar code are translated to their equivalent 'control' key keystroke sequence (13 [0x0d] is translated to Control+M keystrokes as if the user pressed the CTRL, SHIFT, and m keys on the keypad). Additionally, when Translate All is disabled, any control code which has a key-stroke equivalent (enter, tab, escape, backspace, etc.) is output as a keystroke. Any control code without a key-stroke equivalent is dropped.

Character

This is a drop down combo box that contains the control character name. Refer to the Character drop down box for the list of control characters and their names. When a character name is selected from the drop down box, the default text Ignore (drop) is shown and highlighted in the Replacement edit control. Ignore (drop) is highlighted so the user can type a replacement if the control character is not being ignored. Once the user types any character into the Replacement edit control, reselecting the character from the Character drop down box redisplays the default Ignore (drop) in the Replacement edit control.

Replacement

The edit control where the user types the characters to be assigned as the replacement of the control character. Replacements for a control character are assigned by selecting the appropriate character from the Character drop down box, typing the replacement in the Replacement edit control (according to the formats defined above) and then selecting Assign. The assigned replacement is then added to the list box above the Assign button.
For example, if 'Carriage Return' is replaced by Line Feed (by specifying '^J' or '0x0A') in the configuration, the

value 0x0d received in any scanned bar code (or defined in the prefix or suffix) will be replaced with the value 0x0a.
The Wedge then sends Ctrl+J to the receiving application, rather than Ctrl+M.

List Box

The list box shows all user-defined control characters and their assigned replacements. All replacements are enclosed in single quotes to delimit white space that has been assigned.

Delete

This button is grayed unless an entry in the list box is highlighted. When an entry (or entries) is highlighted, and Delete is selected, the highlighted material is deleted from the list box.

Custom Identifiers

The Custom Identifiers button is located on the Data Options tab. Code IDs can be defined by the user. This allows processing parameters to be configured for bar codes that do not use the standard AIM or Symbol IDs or for bar codes that have data embedded at the beginning of the data that acts like a Code ID.

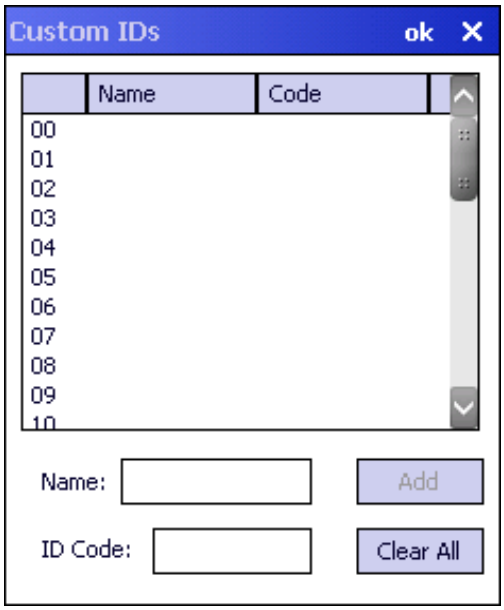
These are called “custom” Code IDs and are included in the Symbology drop down box in the Symbology dialog, unless Enable Code ID is set to None. When the custom Code ID is found in a bar code, the configuration specified for the custom Code ID is applied to the bar code data. The dialog below allows the custom Code IDs to be configured.

It is intended that custom code IDs are used to supplement the list of standard code IDs (if Enable Code ID is set to AIM or Symbol), or to replace the list of standard code IDs (if Enable Code ID is set to Custom).

When Enable Code ID is set to None, custom code IDs are ignored.

Note: Custom symbologies will appear at the end of the list in the Symbology dialog, and are processed at the beginning of the list in the scanner driver itself. This allows custom IDs based on actual code IDs to be processed before the code ID itself.

Note: When Strip: Code ID is enabled, the entire custom Code ID string is stripped (i.e., treated as a Code ID).



Note: After adding, changing and removing items from the Custom IDs list, tap the ok button to save changes and return to the Barcode panel.

Name text box

Name is the descriptor that is used to identify the custom Code ID. Names must be unique from each other; however, the Name and ID Code may have the same value. Name is used in the Symbology drop down box to identify the custom Code ID in a user-friendly manner. Both Name and ID Code must be specified in order to add a custom Code ID to the Custom IDs list.

ID Code text box

ID Code defines the data at the beginning of a bar code that acts as an identifier (the actual Code ID). Both Name and ID Code must be specified in order to add a custom Code ID to the Custom IDs list.

Custom ID Buttons

Add

Entering data into both the Name and ID Code fields enables the Add button. Tap the Add button and the data is added to the next empty location in the Custom ID list.

Insert

Tap on an empty line in the Custom ID list. The Add button changes to Insert. Enter data into both the Name and ID Code fields and tap the Insert button. The data is added to the selected line in the Custom IDs list.

Edit

Double tap on the item to edit. Its values are copied to the text boxes for editing. The Add button changes to Replace. When Replace is tapped, the values for the current item in the list are updated.

Clear All

When no item in the Custom IDs list is selected, tapping the Clear All button clears the Custom ID list and any text written (and not yet added or inserted) in the Name and ID Code text boxes.

Remove

The Clear All button changes to a Remove button when an item in the Custom IDs list is selected. Tap the desired line item and then tap the Remove button to delete it. Line items are Removed one at a time. Contents of the text box fields are cleared at the same time.

Control Code Replacement Examples

Configuration data	Translation	Example Control Character	Example configuration	Translated data
Ignore(drop)	The control character is discarded from the bar code data, prefix and suffix	ESCape	'Ignore (drop)'	0x1B in the bar code is discarded.
Printable text	Text is substituted for Control Character.	Start of TeXt	'STX'	0x02 in a bar code is converted to the text 'STX'.
Hat-encoded text	The hat-encoded text is translated to the equivalent hex value.	Carriage Return	'^M'	Value 0x0d in a bar code is converted to the value 0x0d.
Escaped hat-encoded text	The hat-encoding to pass thru to the application.	Horizontal Tab	'\^I'	Value 0x09 in a bar code is converted to the text '^I'.
Hex-encoded text	The hex-encoded text is translated to the equivalent hex value.	Carriage Return	'0x0A'	Value 0x0D in a bar code is converted to a value 0x0A.
Escaped hex-encoded text	The hex-encoding to pass thru to the application.	Vertical Tab	'\0x0A' or '0\x0A'	Value 0x0C is a bar code is converted to text '0x0A'

Bar Code Processing Examples

The following table shows examples of stripping and prefix/suffix configurations. The examples assume that the scanner is configured to transmit an AIM identifier.

	Symbology				
	All	EAN-128 (]C1)	EAN-13 (]E0)	Intrlv 2 of 5 (]I0)	Code93
Enable	Enabled	Enabled	Enabled	Enabled	Disabled
Min length	1	4	1	1	
Max length	all	all	all	10	
Strip Code ID	Enabled	Enabled	Disabled	Enabled	
Strip Leading	3	0	3	3	
Strip Bar Code Data		'*123'	'1*'	'456'	
Strip Trailing	0	0	3	3	
Prefix	'aaa'	'bbb'	'ccc'	'ddd'	
Suffix	'www'	'xxx'	'yyy'	'zzz'	

Provided that the wedge is configured with the above table, following are examples of scanned bar code data and results of these manipulations.

Bar Code Symbology	Raw Scanner Data	Resulting Data
EAN-128	]C11234567890123	bbb1234567890xxx
EAN-128	]C111234567890123	bbb11234567890xxx
EAN-128	]C1123	< rejected > (too short)
EAN-13	]E01234567890987	ccc]E04567890yyy
EAN-13	]E01231234567890987	ccc]E0234567890yyy

EAN-13	]E01234	ccc]E0yyy
I2/5	]I04444567890987654321	< rejected > (too long)
I2/5	]I04444567890123	ddd7890zzz
I2/5	]I0444	dddzzz
I2/5	]I022245622	ddd45zzz
Code-93	]G0123456	< rejected > (disabled)
Code-93	]G0444444	< rejected > (disabled)
Code-39	]A01234567890	aaa4567890www
Code-39 full ASCII	]A41231234567890	aaa1234567890www
Code-39	]A4	< rejected > (too short)

Rejected bar codes generate a bad scan beep. In some cases, the receipt of data from the scanner triggers a good scan beep (from the external scanner), and then the rejection of scanned bar code data by the processing causes a bad scan beep on the same data.

Length Based Bar Code Stripping

Use this procedure to create symbology rules for two bar codes with the same symbology but with different discrete lengths. This procedure is not applicable for bar codes with variable lengths (falling between a maximum value and a minimum value).

Example 1:

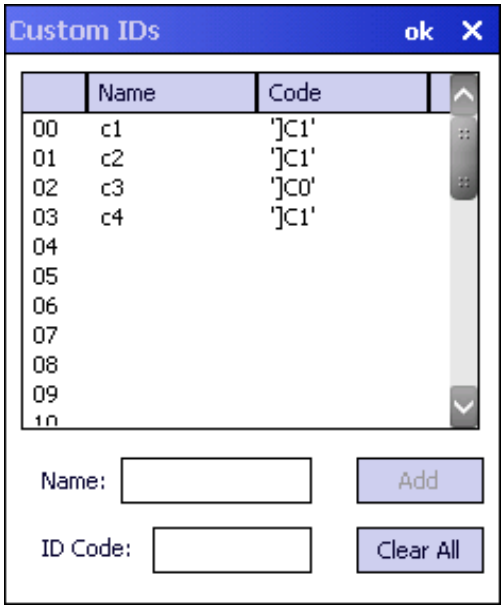
- A normal AIM or Symbol symbology role can be created for the desired bar code ID.
- Next, a custom bar code symbology must be created using the same Code ID as the original AIM or Symbol ID rule and each rule would have unique length settings.

Example 2:

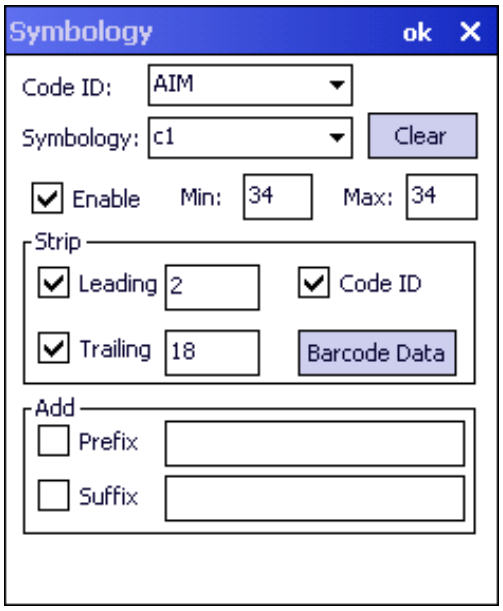
For the purposes of this example, the following sample bar code parameters will be used – EAN 128 and Code 128 bar codes. Some of the bar codes start with '00' and some start with '01'. The bar codes are different lengths.

- 34 character length with first two characters = "01" (strip first 2 and last 18)
- 26 character length with first two characters = "01" (strip first 2 and last 10)
- 24 character length with first two characters = "01" (strip first 2 and last 8). This 24 character bar code is Code 128.
- 20 character length with first two characters = "00" (strip first 0 (no characters) and last 4)

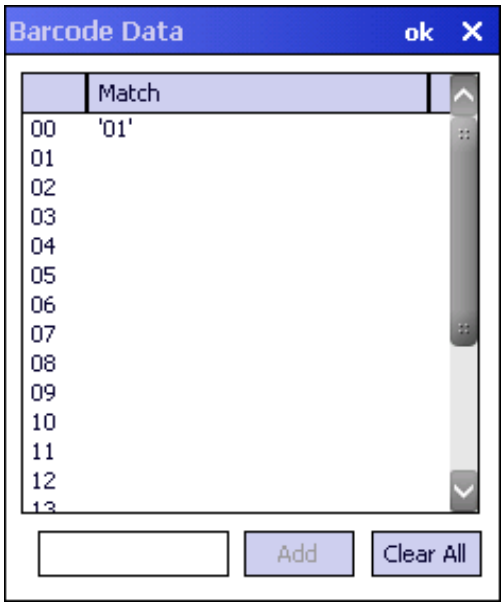
1. On the Data Options tab, set Enable Code ID to AIM.
2. Create four custom IDs, using 1 for EAN 128 bar code and 0 for Code 128 bar code.
   - c1 = Code = ']C1'
   - c2 = Code = ']C1'
   - c3 = Code = ']C0' (24 character bar code is Code 128)
   - c4 = Code = ']C1'



3. AIM custom symbology setup is assigned in the following manner:
   - c1 min length = 34, max length = 34, strip leading 2, strip trailing 18, Code ID enabled, Barcode Data = "01"
   - c2 min length = 26, max length = 26, strip leading 2, strip trailing 10, Code ID enabled, Barcode Data = "01"
   - c3 min length = 24, max length = 24, strip leading 2, strip trailing 8, Code ID enabled, Barcode Data = "01"
   - c4 min length = 20, max length = 20, strip leading 0, strip trailing 4, Code ID enabled, Barcode Data = "00"
4. Add the AIM custom symbologies. Refer to Symbology Settings for instruction.



5. Tap the Barcode Data button.
6. Tap the Add button.
7. Add the data for the match codes.



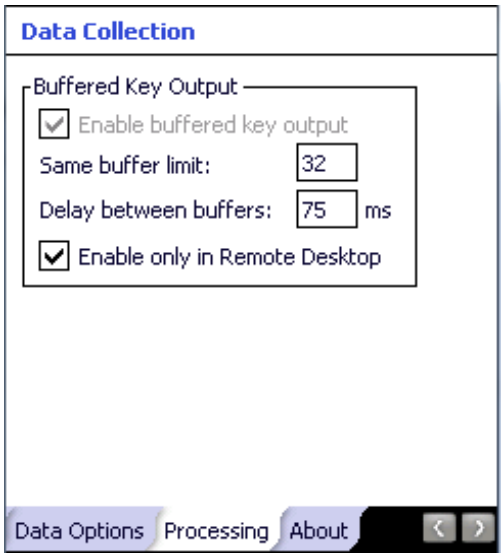
8. Refer to the previous section Bar Code Data Match List (page 8-12) for instruction.
9. Scan a bar code and examine the result.

Processing

The Processing tab contains a user configurable key delay that applies to scanned bar codes as they are input when Remote Desktop is the application with the input focus.

Setting	Default
Enable buffered key output	Enabled and dimmed
Same buffer limit (characters)	32
Delay between buffers	75 ms
Only in Remote Desktop	Enabled

Note: Settings on this panel have no effect when RFTerm is the application with the input focus.



Enable buffered key output

Enabled (checked) and dimmed. The user cannot change this setting.

Same buffer limit

Default is 32 ms. Raise or lower this value as desired.

Delay between (key) buffers

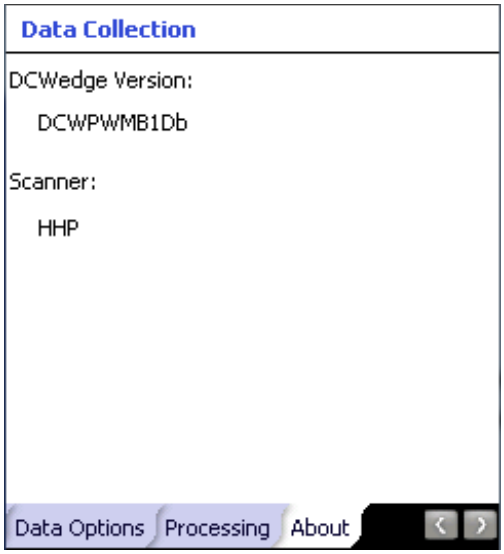
Specifies the number of milliseconds to delay after each character in the scanned bar code is processed as a keystroke. This value may need to be adjusted depending on the network traffic in the environment. The default value is 75 ms. Valid range is from 0 to 9999. A zero value is No Delay between characters.

Enable only in Remote Desktop

The delay specified in Wait between (key) buffers is applied only when Remote Desktop is enabled and is the application with the input focus. When disabled, all keystrokes are delayed by the number of milliseconds specified in Wait between (key) buffers.

About

The About tab lists the version of the Data Collection Wedge (DCWedge) software and the type of laser scan (or imager) engine installed in the MX7 Tecton



Valid scanner / imager types:

- HHP – Hand Held Products 5300 2D Imager
- Honeywell - 4313-TTL (N43XX)
- Honeywell - 7313-TTL (N73XX)
- Symbol – Symbol 955I
- Symbol - Symbol 955E
- Symbol – Symbol SE-1524ER
- No Scanner/None – No scanner installed

Hat Encoding

Hat Encoded Characters Hex 00 through AD

Desired ASCII	Hex Value	Hat Encoded
NUL	0X00	^@
SOH	0X01	^A
STX	0X02	^B
ETX	0X03	^C
EOT	0X04	^D
ENQ	0X05	^E
ACK	0X06	^F
BEL	0X07	^G
BS	0X08	^H
HT	0X09	^I
LF	0X0A	^J
VT	0X0B	^K
FF	0X0C	^L
CR	0X0D	^M
SO	0X0E	^N
SI	0X0F	^O
DLE	0X10	^P
DC1 (XON)	0X11	^Q
DC2	0X12	^R
DC3 (XOFF)	0X13	^S
DC4	0X14	^T
NAK	0X15	^U
SYN	0X16	^V
ETB	0X17	^W
CAN	0X18	^X
EM	0X19	^Y
SUB	0X1A	^Z
ESC	0X1B	^[
FS	0X1C	^\\
GS	0X1D	^]
RS	0X1E	^^
US	0X1F	^ (Underscore)
	0X7F	^?
	80	~^@
	81	~^A
	82	~^B
	83	~^C
IND	84	~^D
NEL	85	~^E
SSA	86	~^F
®	AE	~. (Period)
¯	AF	~/
°	B0	~0 (Zero)
±	B1	~1

Desired ASCII	Hex Value	Hat Encoded
ESA	87	~^G
HTS	88	~^H
HTJ	89	~^I
VTS	8A	~^J
PLD	8B	~^K
PLU	8C	~^L
RI	8D	~^M
SS2	8E	~^N
SS3	8F	~^O
DCS	90	~^P
PU1	91	~^Q
PU2	92	~^R
STS	93	~^S
CCH	94	~^T
MW	95	~^U
SPA	96	~^V
EPA	97	~^W
	98	~^X
	99	~^Y
	9A	~^Z
CSI	9B	~^[
ST	9C	~^\\
OSC	9D	~^]
PM	9E	~^^
APC	9F	~^_ (Underscore)
(no-break space)	A0	~ (Tilde and Space)
¡	A1	~!
¢	A2	~"
£	A3	~#
¤	A4	~$
¥	A5	~%
¦	A6	~&
§	A7	~'
¨	A8	~(
©	A9	~)
ª	AA	~*
«	AB	~+
¬	AC	~,
(soft hyphen)	AD	~- (Dash)
×	D7	~W
Ø	D8	~X
Ù	D9	~Y
Ú	DA	~Z

Hat Encoded Characters Hex AE through FF

Desired ASCII	Hex Value	Hat Encoded
²	B2	~2
³	B3	~3
´	B4	~4
µ	B5	~5
¶	B6	~6
·	B7	~7
¸	B8	~8
¹	B9	~9
º	BA	~:
»	BB	~;
¼	BC	~<
½	BD	~=
¾	BE	~>
¿	BF	~?
À	C0	~@
Á	C1	~A
Â	C2	~B
Ã	C3	~C
Ä	C4	~D
Å	C5	~E
Æ	C6	~F
Ç	C7	~G
È	C8	~H
É	C9	~I
Ê	CA	~J
Ë	CB	~K
Ì	CC	~L
Í	CD	~M
Î	CE	~N
Ï	CF	~O
Ð	D0	~P
Ñ	D1	~Q
Ò	D2	~R
Ó	D3	~S
Ô	D4	~T
Õ	D5	~U
Ö	D6	~V

Desired ASCII	Hex Value	Hat Encoded
Û	DB	~[
Ü	DC	~\\
Ý	DD	~]
Þ	DE	~\^
ß	DF	~_ (Underscore)
à	E0	~`
á	E1	~a
â	E2	~b
ã	E3	~c
ä	E4	~d
å	E5	~e
æ	E6	~f
ç	E7	~g
è	E8	~h
é	E9	~i
ê	EA	~j
ë	EB	~k
ì	EC	~l
í	ED	~m
î	EE	~n
ï	EF	~o
ð	F0	~p
ñ	F1	~q
ò	F2	~r
ó	F3	~s
ô	F4	~t
õ	F5	~u
ö	F6	~v
÷	F7	~w
ø	F8	~x
ù	F9	~y
ú	FA	~z
û	FB	~{
ü	FC	~|
ý	FD	~}
þ	FE	~~
ÿ	FF	~^?

9 Enhanced Launch Utility

Introduction

The launch utility has two functions:

- Process registry based Launch items
- Process script based Launch items

The registry based Launch items are processed before the script based Launch items.

Registry Based Launch Items

Registry based Launch items (documented here) are processed before the Script Based Launch items, see Script Based Launch Items (page 9-4).

The Launch utility can use registry entries to auto-launch Windows CAB files. CAB files exist as separate files from the main installation image, and are copied to the device using ActiveSync, or using the optional SD card. The CAB files are copied into the folder System, which is the internal Flash drive. Then, information is added to the registry, if desired, to make the CAB file auto-launch at startup.

The registry information needed is under the key

HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist

The main subkey is any text, and is a description of the file. Then the values are added:

Value	Need	Data Type	Description
FileName	Required	String	Name of the CAB file, with full path (usually \System)
Installed	Required	DWORD	Starts as 0, changed to 1 when the CAB file is installed
FileCheck	Required	String	File name, with full path, of a file installed by the CAB file. If this file is not found, Launch assumes the CAB file is not installed or memory was lost.
Order	Optional	DWORD	Determines sequence of installation. Order=0 is installed first, order=99 is installed last.
Delay	Optional	DWORD	Delay, in seconds, after this item is installed and before the next one is installed. If the install fails (or is not found) the delay does not occur.
PCMCIA	Optional	DWORD	1=power up PCMCIA/CF slot after installation

The auto-launch process is as follows.

1. The launch utility opens the registry database and reads the list of CAB files to auto-launch.
2. First it looks for **FileName** to see if the CAB file is present.
   - If not, the registry entry is ignored.
   - If it is present, and the **Installed** flag is not set, auto-launch makes a copy of the CAB file (since it gets deleted by installation) and runs the Microsoft utility WCELOAD to install it.
3. If the Installed flag is set, auto-launch looks for the **FileCheck** file.
   - If it is present, the CAB file is installed and that registry entry is complete.
   - If the **FileCheck** file is not present, memory has been lost, and the utility calls WCELOAD to reinstall the CAB file.
4. This process repeats for the next entry in the registry, until all registry entries are analyzed.

Notes:

- To force execution every time, use a FileCheck of “dummy”, which is never found, forcing the item to execute. If an AUTOEXEC.BAT file is found, the terminal runs it by default.
- For persist keys specifying .EXE or .BAT files, the executing process is started, and then Launch continues, leaving the loading process to run independently.
- For other persist keys (including .CAB files), Launch waits for the loading process to complete before continuing. This is important, for example, to ensure that a CAB file is installed before the EXE files from the CAB file are run.

- The Order field is used to force a sequence of events; Order=0 is first, and Order=99 is last. Two items which have the same order are installed in the same pass, but not in a predictable sequence.
- The Delay field is used to add a delay after the item is loaded, before the next is loaded. The delay is given in seconds, and defaults to 0 if not specified. If the install fails (or the file to be installed is not found), the delay does not occur.
- The PCMCIA field is used to indicate that the file (usually a CAB file) being loaded is a radio driver, and the PCMCIA slots must be started after this file is loaded. By default, the PCMCIA slots are off on power up, to prevent the “Unidentified PCMCIA Slot” dialog from appearing. After the drivers are loaded, the slot can be turned on. The value in the PCMCIA field is a DWORD, representing the number of seconds to wait after installing the CAB file, but before activating the slot (a latency to allow the thread loading the driver to finish installation). The default value of 0 means the slot is not powered on. The default values for the default radio drivers (listed below) is 1, meaning one second elapses between the CAB file loading and the slot powering up.
- Note that the auto-launch process can also launch batch files (*.BAT), executable files (*.EXE), registry setting files (*.REG), or sound files (*.WAV). The mechanism is the same as listed above, but the appropriate OS application is called, depending on file type.

Launch Startup Options

The Launch utility uses registry entries to enable or disable startup options. These flags are located in the registry key:

HKEY_LOCAL_MACHINE\Software\LXE\Launch

These can be configured using RegEdit. The options are as follows:

Value	Ship Default	LTK Default	Description
LaunchPSM	1	0	Execute the Persist keys
JumpStart	1	0	Look for and execute JumpStart scripts
LaunchStart	1	0	Execute any auto-install files in \System\Startup
TimeService	0	0	Launches the GrabTime utility as a service, so that the time and date are periodically automatically updated.

It can often be useful to disable these as necessary, to troubleshoot system startup.

Example:

The following example loads and launches RFTerm.

```
;; ------- RFTerm support
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\LXE TE]
"FileName"="\\System\\RFTERM.CAB"
"Installed"=dword:0
"FileCheck"="\\WINDOWS\\LXE\\RFTERM.EXE"
"Order"=dword:11
;; run the app after it has loaded and client device is ready
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\RFTERM]
"FileName"="\\WINDOWS\\LXE\\RFTERM.EXE"
"Installed"=dword:0
"FileCheck"="ALWAYSEXEC"
"Order"=dword:40
"Delay"=dword:1
```

Script Based Launch Items

Note: Script Based Launch items (documented here) are processed after Registry Based Launch items, see Registry Based Launch Items (page 9-1).

The Enhanced (script based) portion of the Launch utility provides several features:

- Launch .CAB file
- Run .EXE file
- Run .EXE file using specified parameters
- Run .BAT file
- Process .REG file
- Copy file, with or without overwriting of existing file
- Delete file
- Create directory
- Remove directory
- Add / Update a registry field
- Delete a registry field
- Add a registry subkey
- Delete a registry key
- Display an on-screen message; message requires OK to continue
- Conditional commands, based on existence of file or folder
- Conditional commands, based on device type
- End block of conditional commands
- Create a shortcut
- Perform a Suspend/Resume (Restart is not useful in this context).

The script developer has the option of pausing script file execution until the current action completes, or continuing script file processing. The script developer is also able to pause for a specified number of milliseconds between commands.

The utility also processes .REG files, using the same format as the legacy Launch Utility. It does this by calling the RegLoad utility. It can also process .BAT files, by calling the Command Prompt utility.

- By default, Enhanced Launch processes both registry entries and scripts, if present. There are registry settings to enable/disable processing of both types of files.
- Script files may have the extension .CLD (for cold boot) or .WRM (for warm boot.) With this extension, they may be clicked to execute from the File Explorer. When clicked directly, the extensions do not matter (a script ending in .CLD does not have to be preceded by a suspend/resume).

Enhanced Launch Utility Use

The Enhanced Launch Utility can be used at OS startup to execute commands from a script file or to launch programs. The user can configure scripts or registry entries for different operation after Warm Boot and Restart. Use of scripts and registry entries is documented in the following sections.

File Names

From a Restart, Launch tries to find the file JmpStart.cld, but from a Warm Boot it looks for JmpStart.wrm. The Launch program can also be run manually. Unless it is given a file as part of the command line it tries to run Launch.txt. The script file may be in ASCII or Unicode.

When trying to find a script file, Launch looks in the following locations (in sequence):

1. root directory of the Flash (\System\JmpStart.xxx)
2. root directory of the SD card (\SD Card\JmpStart.xxx).

In addition, a script file can be written (with a cld or .wrm extension), and can be double-clicked to run from the File Explorer.

Command line structure

Each command takes up one line. Every command uses the format:

```
COMMAND,PARAMETER1,PARAMETER2,...etc.
```

Parameters are separated by a single comma. If a parameter requires a comma within it, the whole parameter must be enclosed in quote marks ("). Extra spaces are ignored between the comma and the next parameter.

For Example

To delete a file called **Ive, got, commas, in, my, name.txt**, use the command

```
delete,"Ive, got, commas, in, my, name.txt".
```

Enclosing quotes are used to allow commas inside a parameter, but are removed prior to executing the command. Thus, delete,deleteme.txt is the same as delete,“deleteme.txt”. If a parameter requires a quote mark within it, the whole parameter must first be enclosed within quote marks, and the required quote mark is represented by two quote marks (""). For example, to place the message **This is how you display “quote marks**” **on the screen**, use the command

```
message,This is a heading,"This is how you display ""quote marks""".
```

The case of a command is ignored, so delete is the same as DELETE and DeLeTe.

Comments

Any line that starts with a semicolon (;), a slash (‘/’) or an asterisk (*) is treated as a comment, and ignored by Launch.

Launch also ignores any extra parameters (more than the required number) in a command. It is not recommended that comments be placed on the end of lines as any future changes could render your script files incompatible.

Blank lines are also ignored.

Commands Supported by Launch

Copy	ElseIfFile	IfFile	Mkdir	
Delete	EndIf	IfTerm	Rmdir	
DelRegData	EndIfFile	Launch	SetRegData	
DelRegKey	EndIfTerm	LaunchCmd	SetRegKey	
ElseIf	FCopy	Message	Shortcut	

The commands supported by Launch are detailed below. Square brackets indicate that a parameter is optional. Characters in italics represent a variable, and not a literal.

Copy

Description — Copies a file but does not overwrite an existing file.

Syntax — **Copy**,*source-file,destination-file*

Parameters — *source-file*: The file to be copied, including its path.
destination-file: The destination path and filename.

Example —
```
copy,\Storage Card\MyData.dat,\Temp\MyData.dat
```

Notes — If the destination file already exists, it is not overwritten, and no error is given.
If the source file is blank, a zero-byte file is created.

Delete

Description — Deletes the specified file.

Syntax — **Delete**,*source-file*

Parameter — *source-file*: The file to be deleted, including its path.

Example —
```
delete,\Temp\MyData.dat
```

DelRegData

Description — Deletes a specified registry data field.

Syntax — **Delregdata**,*key,subkey,field*

Parameter — *key*: The abbreviated major registry key where you want to delete a field. Can be one of:
- **cr** or **hkcr** (HKEY_CLASSES_ROOT)
- **cu** or **hkcu** (HKEY_CURRENT_USER)
- **lm** or **hklm** (HKEY_LOCAL_MACHINE).

The case of *key* does not matter.

subkey: The subkey that holds the field you want to delete.
field: The field that you want to delete.

Example —
```
delregdata,LM,Software\WidgetsPlc\OurApp,AppName
```

Notes — An error isn't displayed if you specify a non-existent field, but is displayed if you specify a non-existent key or subkey.

DelRegKey

Description	Deletes a specified registry subkey.
Syntax	**Delregkey**,*key*,*subkey*
Parameter	*key*: The abbreviated major registry key where you want to delete the subkey. Can be one of: • **cr** or **hkcr** (HKEY_CLASSES_ROOT) • **cu** or **hkcu** (HKEY_CURRENT_USER) • **lm** or **hklm** (HKEY_LOCAL_MACHINE). The case of *key* does not matter. *subkey*: The subkey you want to delete.
Example	`delregkey,LM,Software\WidgetsPlc\OurApp`
Notes	Deletes the specified subkey and all of its contents (if any).

ElseIf

Description	Begins conditional command block, executed only if the previous IF command was FALSE.
Syntax	ElseIf
Parameter	None
Example	See IfFile (page 9-9).
Notes	Results are unpredictable when ElseIf is not paired properly with If… command.

ElseIfFile

Description	Begins conditional command block executed only if the file specified in the previous IfFile does not exist.
Syntax	ElseIfFile
Parameter	None
Example	See IfFile (page 9-9).
Notes	Results are unpredictable if not paired properly with IfFile command.

EndIf

Description	Ends conditional command block begun with the previous IF command.
Syntax	EndIf
Parameter	None
Example	See IfFile (page 9-9).
Notes	Results are unpredictable if not paired properly with If... command.

EndIfFile

Description	Ends conditional command block begun with the previous IF command.
Syntax	EndIfFile
Parameter	None
Example	See IfFile (page 9-9).
Notes	Results are unpredictable if not paired properly with IfFile command.

EndIfTerm

Description	Ends conditional command block executed only if the device type specified in IfTerm matches.
Syntax	EndIfTerm
Parameter	None
Example	See IfTerm (page 9-9).
Notes	Results are unpredictable if not paired properly with IfTerm command.

FCopy

Description	Copies a file, overwriting any existing file.
Syntax	**fcopy**,*source-file,destination-file*
Parameters	*source-file*: The file to be copied, including its path *destination-file*: The destination path and filename
Example	`fcopy,\Storage Card\MyData.dat,\Temp\MyData.dat`
Notes	If the destination file already exists it is overwritten. If the source file is blank, a zero-byte file is created.

IfFile

Description	Begins the conditional execution of a block of commands only if the specified file exists.
Syntax	**IfFile**,*file*
Parameter	*file*: The path and filename to determine if the commands should be executed

Example	`IfFile,\System\MyData.dat`
	any number of commands, executed if file exists
	`ElseIfFile`
	any number of commands, executed if file does not exist
	`EndIfFile`

Notes	If the file already exists the commands are executed. This test does not care if file is a file or directory. Nesting is supported.

IfTerm

Description	Begins the conditional execution of a block of commands only if the terminal matches the specified terminal type.
Syntax	**IfTerm**,*terminal*
Parameter	*terminal*: The terminal type to determine if the commands should be executed

Example	`IfTerm,MX8`
	any number of commands
	`EndIfTerm`

Notes	If the terminal type is identical (not case-dependent) the commands are executed. Nesting with IfFile is supported. Nesting with IfTerm is meaningless.

Launch

Description	Runs a program.
Syntax	**Launch**,*program,wait-code*
Parameter	*program*: The full path and filename of the program to be run. *wait-code*: Tells Launch how to behave when the program is running. **w(ait)** causes Launch to stop processing the script until the program has finished executing. **c(ontinue)** makes Launch continue processing the script while the program is executing.
Example	`launch,\Windows\Calc.exe,w`
Notes	This differs from **LaunchCmd** in that **Launch** has no parameters.

LaunchCmd

Description	Runs a program with arguments.
Syntax	**Launchcmd**,*program,arguments,wait-code*
Parameters	*program*: The full path and filename of the program to be run. *arguments*: The command line arguments for program. *wait-code*: Tells Launch how to behave when the program is running. **w(ait)** causes Launch to stop processing the script until the program has finished executing. **c(ontinue)** makes Launch continue processing the script while the program is executing.
Example	`launchcmd,\Windows\Pword.exe,\My documents\Doc1.doc,w`
Notes	This differs from **Launch** in that **LaunchCmd** allows parameters.

Message

Description	Displays a message on the screen.
Syntax	**Message**,*message-title,message-body*
Parameters	*message-title*: A heading for the message. Can be left empty. *message-body*: The main body of the message. To display a message over multiple lines, use the \n character combination at the end of each line. To display a single backslash use two together (\\).
Example	`message,This is a message,"This is the first line,\nand this is the second"`
Notes	Displaying a message pauses the execution of the script file until the message is OK'd. This is displayed with a modal dialog.

Mkdir

Description	Creates a directory.
Syntax	**Mkdir**,*dir*
Parameters	*dir*: The full path and name of the directory to be created.
Example	`mkdir,\Program Files\MyApp`
Notes	A new directory cannot be created if its parent directory doesn't exist. For example, to create a directory called \MyApp with a subdirectory called SubDir1, use mkdir,\MyApp followed by mkdir,\MyApp\SubDir1.

Rmdir

Description	Removes a directory.
Syntax	**Rmdir**,*dir*
Parameters	*dir*: The full path and name of the directory to be removed.
Example	`rmdir,\Program Files\MyApp`
Notes	A directory cannot be removed if it contains files or subdirectories.

SetRegData

Description	Adds or updates a data field in the registry.
Syntax	**Setregdata**,*key,subkey,type,field,data[,data2][,data3]...*
Parameter	*key*: The abbreviated major registry key where you want to create/update the subkey. Can be one of: • **cr** or **hkcr** (HKEY_CLASSES_ROOT) • **cu** or **hkcu** (HKEY_CURRENT_USER) • **lm** or **hklm** (HKEY_LOCAL_MACHINE). The case of *key* doesn't matter *subkey*: The subkey you want to create/update a field in. *type*: The data type of the field you wish to create/update. Can be s (for string value), dd (for decimal value), dx (for hexadecimal value) or b (for binary value). The case of *type* doesn't matter. If you're altering an existing field, *type* can be different from the current type. *field*: The name of the new field to be created/updated. *data*: The value of the field being created. This depends on the *type* of field. Binary fields can have many values (up to 2000 bytes). In this case the data field holds the number of bytes in the binary field, and each byte is given as a subsequent parameter in hexadecimal *(data2, data3* etc.).

Example	`Setregdata,LM,WidgetsPlc\Info,s,AppName,The Widget Program`
	`Setregdata,LM,WidgetsPlc\Info,dx,HexField,FA5B`
	`Setregdata,LM,WidgetsPlc\Info,b,5,d3,62,58,f1,9c`

SetRegKey

Description	Adds a sub key to the registry.
Syntax	**Setregkey**,*key,subkey*
Parameters	*key*: The abbreviated major registry key where you want to create the subkey. Can be one of: • **cr** or **hkcr** (HKEY_CLASSES_ROOT) • **cu** or **hkcu** (HKEY_CURRENT_USER) • **lm** or **hklm** (HKEY_LOCAL_MACHINE). The case of *key* doesn't matter. *subkey*: The subkey you want to create.
Example	`Setregkey,LM,Software\MyApp`
Notes	Attempting to create a key that already exists does not cause an error.

Shortcut

Description	Creates a shortcut.
Syntax	**Shortcut**,*name,target*
Parameters	*name*: The path and name of the shortcut file. The file name must end in .lnk for Windows to recognize it as a shortcut. *target*: The target of the shortcut. If the target has a space in it quote marks must be used (see Command Line Structure section and example below).
Example	`shortcut,\Program Files\Widget.lnk,"""\My App\Widget.exe"""`
Notes	No validation is performed on *target* to be sure it is executable.

Launch Error Messages

Launch displays a message if it encounters an error during the processing of a script. It is possible to get cascading error messages, as Launch does not stop processing the script if it encounters an error. An example of this would be a failure creating a directory causing the failure of all files copied to that directory.

Here is a list of the possible error messages that could be given:

Error Message	Given by	Description
Bad wait code wait-code	Launch LaunchCmd	The wait-code wasn't recognized
Directory Creation Failed error-code	MkDir	There was a problem encountered creating the directory
Directory Removal Failed error-code	RmDir	There was a problem encountered removing the directory
Error reading script file	-	An error occurred reading the script file.
File Copy Failed error-code	Copy Fcopy	There was a problem encountered copying the file
File Delete Failed error-code	Delete	There was a problem encountered deleting the file
Invalid Command: command	-	The command wasn't recognized
Invalid Data Length data	SetRegData	Tried to set more than 2000 byte values in a binary field
Invalid Data Type type	SetRegData	The value of the type parameter is invalid
Invalid decimal data data	SetRegData	The data field doesn't contain decimal data
Invalid hex data data	SetRegData	The data field doesn't contain hexadecimal data
Invalid Registry Key key	DelRegData DelRegKey SetRegData DelRegKey	The key parameter to the command has not been recognized
Parms: Invalid Create Directory	MkDir	Not enough parameters were supplied.
Parms: Invalid Create Registry Key	SetRegKey	Not enough parameters were supplied.
Parms: Invalid Create Shortcut	Shortcut	Not enough parameters were supplied.
Parms: Invalid Delete Registry Data	DelRegData	Not enough parameters were supplied.
Parms: Invalid Delete Registry Key	DelRegKey	Not enough parameters were supplied.
Parms: Invalid File Copy	Copy Fcopy	Not enough parameters were supplied.
Parms: Invalid File Delete	Delete	Not enough parameters were supplied.
Parms: Invalid Program Name	Launch LaunchCmd	Not enough parameters were supplied.
Parms: Invalid Remove Directory	RmDir	Not enough parameters were supplied.
Parms: Invalid Set Registry Data	SetRegData	Not enough parameters were supplied.
Parms: Invalid User Message	Message	Not enough parameters were supplied.
Program Launch couldn't get Exit-Code error-code	Launch LaunchCmd	There was a problem getting the exit status of the program.
Program Launch Failed error-code	Launch LaunchCmd	There was a problem executing the program.
Registry Key Create Failed error-code	SetRegKey	There was a problem creating the registry key given.
Registry Key Delete Failed error-code	DelRegKey	There was a problem deleting the registry key given.

Error Message	Given by	Description
Registry Value Delete Failed error-code	DelRegData	There was a problem deleting the registry data. Most likely a bad sub-key.
Registry Value Set Failed error-code	SetRegData	There was a problem setting the registry data. Most likely a bad subkey.
Shortcut Creation Failed error-code	Shortcut	There was a problem encountered creating the shortcut.
Unable to open file script-file	-	There was a problem opening the script-file. This message is only displayed when manually running Launch.

Example Script File

```
iffile,\System\applock.cab
launchcmd,\Windows\wceload.exe,"/noaskdest /noui \System\applock.cab",w
launch,\Windows\applockprep.exe,c
endiffile
launchcmd,\Windows\wceload.exe,"/noaskdest /noui \System\wedge.cab",w
iffile,\System\summit.cab
launchcmd,\Windows\wceload.exe,"/noaskdest /noui \System\summit.cab",w
endiffile
iffile,\System\RFTerm.cab
launchcmd,\Windows\wceload.exe,"/noaskdest /noui \System\RFTerm.cab",w
endiffile
iffile,\System\Java.cab
launchcmd,\Windows\wceload.exe,"/noaskdest /noui \System\Java.cab",w
launchcmd,\Windows\wceload.exe,"/noaskdest /noui \Windows\Jeode.cab",w
endiffile
launch,\System\regrest.exe,w
coldboot
```

10 Enabler Installation and Configuration

Introduction

This section discusses Honeywell supported features of Wavelink Avalanche Mobile Device Servers. This section is split into three basic areas:

- Installation
- User Interface
- Enabler Configuration

Installation

To use the Wavelink Avalanche MC System, the following items are required:

- A desktop or laptop PC on which to install the Avalanche MC Console.
- A desktop or laptop PC on which to install the Avalanche Mobile Device Server (this can be the same PC where the Avalanche MC Console is installed).
- Wavelink Avalanche MC Console 4.2 or later.
- A Wavelink Device License for each client device.

To use Avalanche Remote Control, the following additional items are required:

- Wavelink Remote Control plug-in, 2.0 or later
- A Wavelink Remote Control License for each client device

Installing the Enabler on Mobile Devices

The Enabler for a MX7 Tecton (with a Windows Mobile operating system) can update the operating system if the MX7 Tecton has a storage card. The presence of a storage card is one of the package selection criteria.

Mobile devices have the Avalanche Enabler installation files loaded, but not installed, on the mobile device when it is shipped. The installation files are located in the \System folder.

Note: Important: If the user is NOT using Wavelink Avalanche to manage their mobile device(s), the Enabler should not be installed on the mobile device(s). Doing so results in unnecessary delays when booting the device.

The Avalanche Enabler installation file HSM_ENABLER_CAB is loaded on the MX7 Tecton by Honeywell; however, the device is not configured to launch the Enabler installation file automatically. The installation application must be run manually the first time Avalanche is used.

After the installation application is manually run, the Enabler will, by default, be an auto-launch application.

This behavior can be modified by accessing the Avalanche Update Settings panel through the Enabler Interface.

The RMU.CE.CAB file is placed on the device during manufacturing in the \System\RMU folder.

During the Enabler installation process, the Enabler checks for the RMU.CE.CAB file in the \System folder.

- If present, it assumes the RMU.CE.CAB file is already installed and continues.
- If the file RMU.CE.CAB file is not present, it looks for the file in the \System\RMU folder.
- If present, the Enabler copies the file to the \System folder and installs it.

At this point, the OS will automatically install the RMU (Remote Management Utility) after the MX7 Tecton reboots.

Enabler Uninstall Process

To remove the Avalanche Enabler from the MX7 Tecton:

- Delete the Avalanche folder located in the \System directory.
- Warm boot the MX7 Tecton.

The Avalanche folder cannot be deleted while the Enabler is running. See *Stop the Enabler Service*.

If sharing errors occur while attempting to delete the Avalanche folder, warm boot the MX7 Tecton, immediately delete the Avalanche folder, and then perform another warm boot.

Stop the Enabler Service

To stop the Enabler from monitoring for updates from the Mobility Center Console:

1. Open the Enabler Settings Panels by tapping the Enabler icon on the MX7 Tecton desktop.
2. Select **File > Settings**.
3. Select the **Preferences** tab.
4. Select **Do not monitor** to prevent automatic monitoring upon Startup.
5. Select **Exit Application** for an immediate shutdown of all Enabler update functionality upon exiting the user interface.
6. Tap the **OK** button to save the changes.
7. Reboot the MX7 Tecton if necessary.

Update Monitoring Overview

There are three methods by which the Enabler on the MX7 Tecton can communicate with the Mobile Device Server running on the host machine.

- Wired via a serial cable between the Mobile Device Server PC and the MX7 Tecton.
- Wired via a USB connection, using ActiveSync, between the Mobile Device Server PC and the MX7 Tecton.
- Wirelessly via the MX7 Tecton radio and an access point

After installing the Enabler on the MX7 Tecton the Enabler searches for a Mobile Device Server, first by polling all available serial ports and then over the wireless network.

The Enabler running on the MX7 Tecton will attempt to access COM1, COM2, and COM3. “Agent not found” will be reported if the Mobile Device Server is not located or a serial port is not present or available (COM port settings can be verified using bar code wedge panels on the MX7 Tecton).

The wireless connection is made using the default wireless [radio] interface on the mobile device therefore the MX7 Tecton must be actively communicating with the network for this method to succeed.

If a Mobile Device Server is found, the Enabler automatically attempts to apply all wireless and network settings from the active profile. The Enabler also automatically downloads and processes all available packages.

If the Enabler does not automatically detect the Mobile Device Server, the IP address of the Mobile Device Server can be entered on the Connect tab of the Enabler setup. See Enabler Configuration (page 10-4) for details.

Mobile Device Wireless and Network Settings

Once the connection to the Mobile Device Server is established, the MX7 Tecton Enabler attempts to apply all network and wireless settings contained in the active profile.

The success of the application of settings is dependent upon the local configuration of control parameters for the Enabler.

These local parameters cannot be overridden from the Avalanche MC Console.

The default Enabler adapter control settings are:

- Manage network settings – enabled
- Use Avalanche network profile – enabled
- Manage wireless settings – disabled for Windows CE devices

To configure the Avalanche Enabler management of the network and wireless settings:

1. Open the Enabler Settings Panels by tapping the Enabler icon on the desktop.
2. Select **File > Settings**.
3. Select the **Adapters** tab.
4. Choose settings for the **Use Manual Settings** parameter.
5. Choose settings for Manage Network Settings, Manage Wireless Settings and Use Avalanche Network Profile.
6. Tap the OK button to save the changes.
7. Reboot the device.

Preparing a Device for Remote Management

Two additional utilities are necessary for remote management.

Remote Management Utility (RMU)

The Remote Management Utility (RMU) must be installed on all mobile devices first – then you can control mobile device reboot, storage RAM adjustment, real-time updates and Avalanche Enabler properties.

If in doubt, verify RMU.CE.CAB exists in the \System folder. If the RMU.CE.CAB file is present when the Enabler is installed, the RMU is also installed.

Important: If the OS package includes double-byte Asian fonts, the storage RAM property of the RMU must be higher than the default value (40MB).

If the amount of storage RAM is too low, the Enabler returns a “Mobile unit out of resources” error.

To determine the minimum value required, inspect the RMU.StorageRAM>=*nn* parameter in the Criteria field for the OS package. Generally, this setting should be approximately 40 MB above the amount of RAM in use on the device for a standard OS and 50MB above the amount of RAM in use for an OS with Asian fonts.

For example, if after installing all the software, the device shows 5MB in use, this setting should be about 45MB for a standard OS, 55 MB for an Asian font OS.

Wireless Configuration Application (WCA)

Use the Wireless Configuration Application (WCA) when you want to remotely manage the Summit client device. This utility is downloaded and installed in addition to the Remote Management Utility. The WCA is included when the Summit radio driver software is updated. The WCA is automatically installed when the radio driver is updated.

User Interface

The Enabler can be configured and controlled manually through the user interface on the MX7 Tecton. This section details the functionality that can be controlled by the user or system administrator.

Screen displays shown in this section are designed to present the end-user with information graphically.

Information on the screen displays may be split between one or many tabbed panels.

Standard Avalanche Enabler parameters that are not supported may be missing or dimmed (visible but unable to be edited) on the tabbed panels or screen displays.

Enabler Configuration

Depending on the version of the Enabler running on the MX7 Tecton, the desktop Enabler icon may look like one of the following:

 or  Enabler Settings Icon

The Enabler user interface application is launched by tapping either the Enabler Settings icon on the desktop or Taskbar or by selecting Avalanche Enabler from the Programs menu.

The opening screen presents the MX7 Tecton user with the connection status and a navigation menu.

Note: Some parameters and features described in this section may not be available if you do not have the latest version of the Enabler. Contact Technical Assistance *(page 16-1) for upgrades.*

File Menu Options

Connect

The Connect option under the File menu allows the user to initiate a manual connection to the Mobile Device Server. The connection methods, by default, are wireless and COM connections. Any updates available will be applied to the MX7 Tecton immediately upon a successful connection.

Scan Config

The Scan Configuration feature is not supported. The Scan Config option under the File menu allows the user to configure Enabler settings using a special bar code that can be created using the Avalanche MC Console utilities. Refer to the *Wavelink Avalanche Mobility Center User Guide* for details.

Settings

The Settings option under the File menu allows the MX7 Tecton user to access the control panel to locally configure the Enabler settings. The Enabler control panel is, by default, password protected.

The default Settings password is **system**. The password is not case-sensitive.

Avalanche Update using File > Settings

Use these menu options to setup the Avalanche Enabler on the MX7 Tecton. Change settings and save the changes (reboot) before connecting to the network.

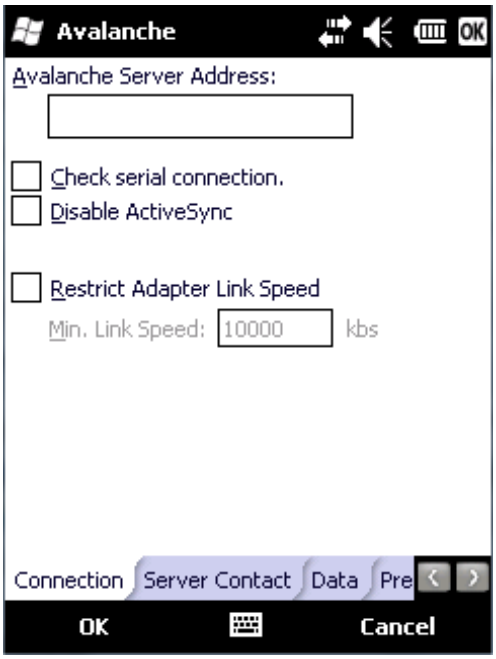
Alternatively, the Mobile Device Server can be disabled until needed (refer to the *Wavelink Avalanche Mobility Center User's Guide* for details).

Menu Options

Note: Your MX7 Tecton screen display may not be exactly as shown in the following menu options. Contact Technical Assistance *(page 16-1) for version information and upgrade availability.*

Option	Function
Connection	Enter the IP Address or host name of the Mobile Device Server. Set the order in which serial ports or RF connections are used to check for the presence of the Mobile Device Server.
Execution	*Not available in this release*. Use AppLock (Application Locking) (page 6-1), which is resident on each device.
Server Contact	Setup synchronization, scheduled Mobile Device Server contact, suspend and reboot settings.
Data	Control when data is transferred between the device and the Mobile Device Server.
Preferences	Set options for Enabler startup or shutdown and logging.
Taskbar	Set options for Taskbar.
Scan Config	This option allows the user to configure Enabler settings using a special bar code that is created by the Avalanche MC Console. *Scan Config not currently supported.*
Display	Set up the Windows display at startup, on connect and during normal mode. The settings can be adjusted by the user.
Shortcuts	Add, delete and update shortcuts to user-allowable applications.
SaaS	Configure the Enabler to connect with Avalanche on Demand.
Adapters	Enable or disable network and wireless settings. Select an adapter and switch between the Avalanche Network Profile and manual settings.
Status	View the current adapter signal strength and quality, IP address, MAC address, SSID, BSSID and Link speed. The user cannot edit this information.

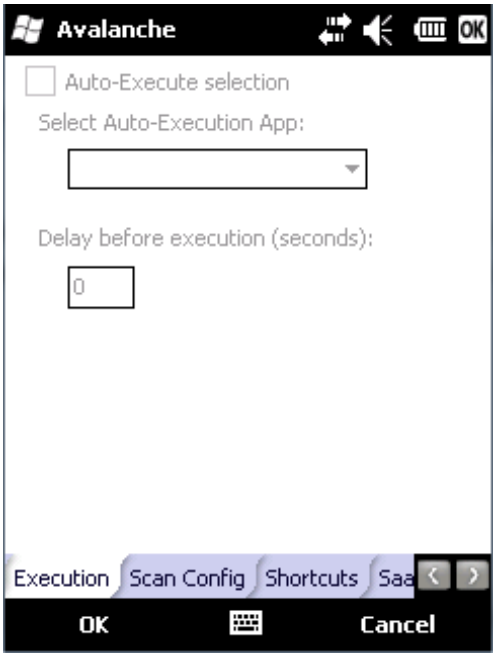
Connection



Setting	Function
Avalanche Server Address	Enter the IP Address or host name of the Mobile Device Server assigned to the MX7 Tecton.
Check Serial Connection	Indicates whether the Enabler should first check for serial port connection to the Mobile Device Server before checking for a wireless connection to the Mobile Device Server.
Disable ActiveSync	Disable ActiveSync connection with the Mobile Device Server.
Restrict Adapter Link Speed	Default is disabled. Minimum Link Speed dimmed.

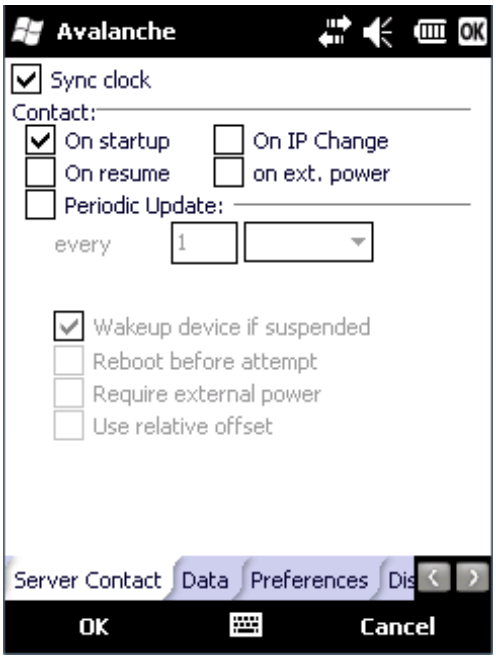
Execution

Note the dimmed options on this MX7 Tecton panel. This menu option is designed to manage downloaded applications for automatic execution upon startup.



Setting	Function
Auto-Execute Selection	An application that has been installed with the Avalanche Management system can be run automatically following each boot.
Select Auto-Execute App	The drop-down box provides a list of applications that have been installed with the Avalanche Management System.
Delay before execution	Time delay before launching Auto-Execute application.

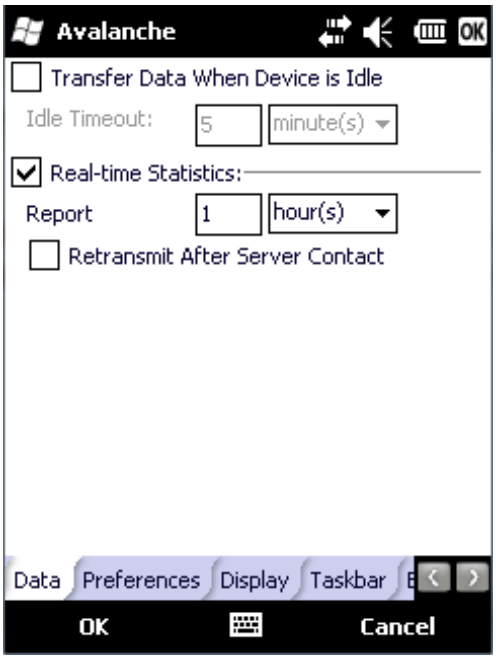
Server Contact



Note: Your MX7 Tecton screen display may not be exactly as shown above. Contact Technical Assistance (page 16-1) for upgrade availability and version information.

Setting	Function
Sync Clock	Reset the time on the MX7 Tecton based on the time on the Mobile Device Server host PC.
Contact	On Startup – Connect to the Mobile Device Server when the Enabler is accessed.
	On Resume – Connect to the Mobile Device Server when resuming from Suspend mode.
	On IP Change – Connect to the Mobile Device Server when the IP address of the MX7 Tecton changes.
	On Ext. Power – Initiate connection to the Mobile Device Server when the device is connected to an external power source, such as based on a docking event.
Periodic Update	Allows the administrator to configure the Enabler to contact the Mobile Device Server and query for updates at a regular interval beginning at a specific time.
Wakeup device if suspended	If the time interval for periodic contact with the Mobile Device Server occurs, a mobile device that is in Suspend Mode can wakeup and process updates.
Reboot before attempt	Reboot mobile device before attempting to contact Mobile Device Server.
Require external power	Only connect when the mobile device has external power.
Use relative offset	Dimmed.

Data

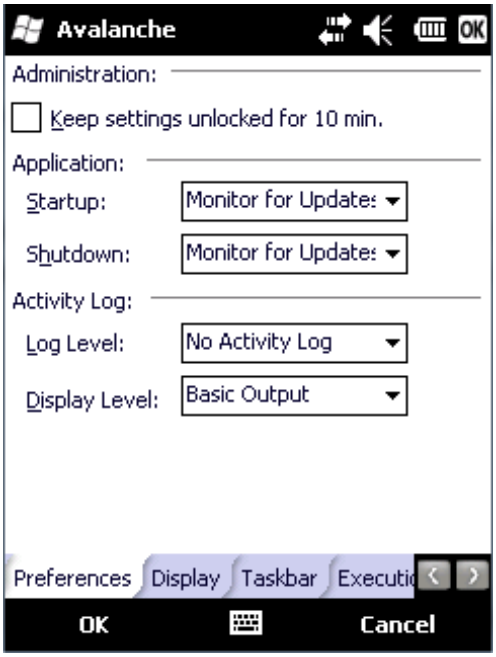


The Data tab controls when data is transferred between the MX7 Tecton and the Mobile Device Server.

Setting	Function
Transfer Data When Device is Idle	When enabled, periodic updates from the Mobile Device Server are postponed until the MX7 Tecton has been idle for the specified period of time. The default is disabled.
Idle timeout	Specify the length of time the device must be idle before a periodic update can run, used when the parameter above is enabled.
Real-time Statistics	When checked, the statistics are transmitted over the network by the Enabler.
Report	Specifies the Report Interval, how frequently the Enabler reports statistics to the Mobile Device Server.
Retransmit After Server Contact	Specifies if the device sends statistics to the Mobile Device Server immediately following a connection to the server.

Preferences

For best results, use AppLock to manage the taskbar. AppLock (Application Locking) (page 6-1) is resident on each mobile device.



Administration

By default, *Keep settings unlocked for 10 minutes* is disabled (check box is blank).

Application

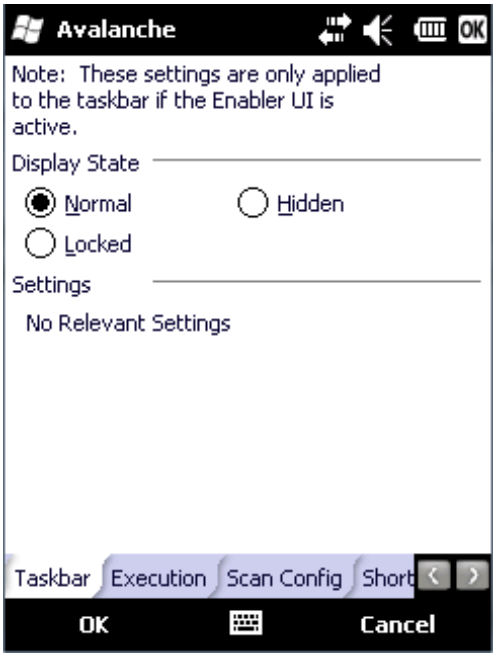
Setting	Function
Startup	Behavior of the Enabler when the MX7 Tecton boots up. The default is Monitor for Updates. • Do not Monitor - When the device boots, do not launch the Enabler application and do not attempt to connect to the Mobile Device Server. • Monitor for Updates - Attempt to connect to the Mobile Device Server and process any updates that are available. Do not launch the Enabler application. • Launch User Interface - Attempt to connect to the Mobile Device Server and process any updates that are available. Launch the Enabler application.
Shutdown	Behavior of the monitor when the Enabler is exited. The default is Monitor for Updates. • Monitor for Updates - Attempt to connect to the Mobile Device Server and process any updates that are available. Do not launch the Enabler application. • Exit Application - Terminates the monitor (requires successful password entry if a password has been configured).

Activity Log

Setting	Function
Log Level	Use this option to control the level of detail recorded in the log file. The default is No Activity Log. • No Activity Log - No log file is written. • Critical - Only critical errors written to the log files. • Error - Communication or configuration problems are written to the log file along with critical messages. • Warning - Possible operation problems are written to the log file along with critical and error messages. • Info - Operational information is written to the log file. • Debug - The most detailed log file.
Display Level	Use this option to control the level of detail shown on the main Enabler screen. The default is Basic Output. • Basic Output - General information is displayed. • Critical - Critical errors are displayed in addition to those above. • Error - Communication or configuration problems are displayed in addition to those above. • Warning - Possible operation problems are displayed in addition to those above. • Info - Operational information is displayed in addition to those above. • Debug - The most detailed list is displayed..

Taskbar

For best results, use AppLock to manage the taskbar. AppLock (Application Locking) (page 6-1) is resident on each mobile device.

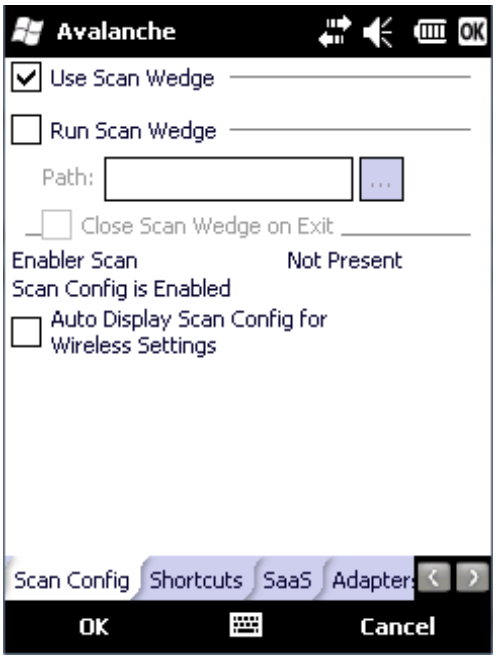


The Display State options control the appearance of the taskbar while using the Enabler interface.

- Normal - taskbar is visible, taskbar icons function normally.
- Hidden - taskbar is not displayed
- Locked - taskbar is visible, but most icons are hidden or for information only.

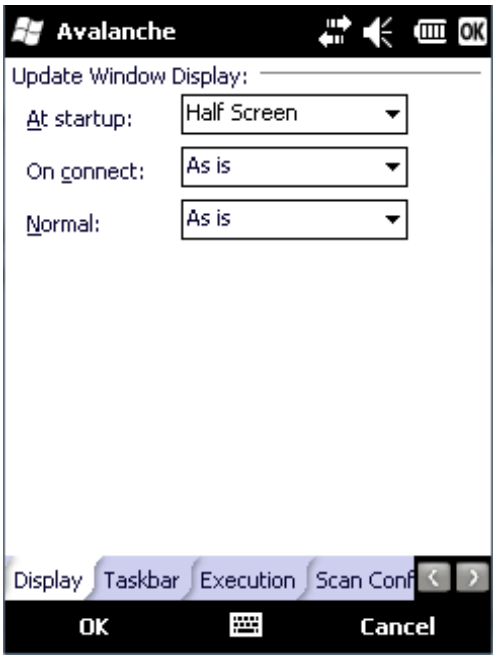
Scan Config

For best results, use eXpress Config and eXpress Scan for this function. eXpress Scan is included with the updated MX7 Tecton enablers.



Scan Config functionality is a standard option of the Wavelink Avalanche MC system but is *not currently supported* on the MX7 Tecton.

Display

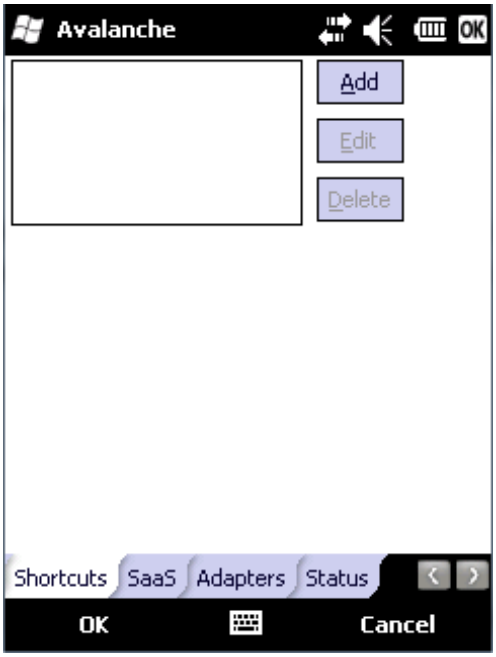


The user interface for the Enabler can be configured to dynamically change based on the status of the MX7 Tecton connection with the Mobile Device Server.

Setting	Function
At startup	Default is Half Screen. Options are Half screen, Hidden or Full screen.
On connect	Default is As Is. Options are As is, Half screen, or Full screen.
Normal	Default is As Is. Options are Half screen, Hidden or As Is.

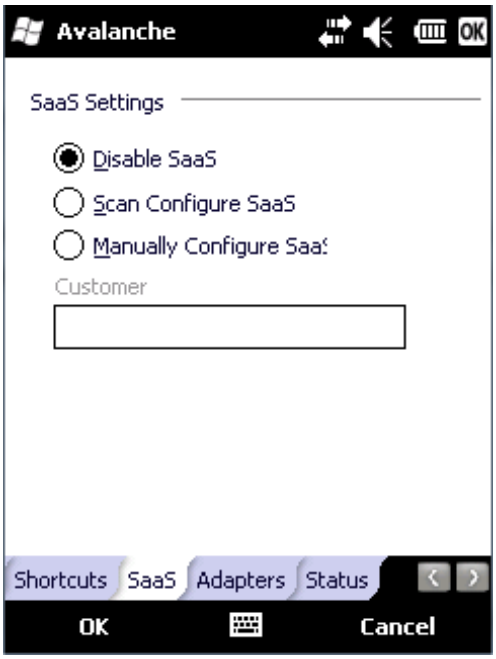
Shortcuts

For best results, use AppLock for this function. AppLock (Application Locking) (page 6-1) is resident on each mobile device.



Configure shortcuts to other applications on the MX7 Tecton. Shortcuts are viewed and activated in the Programs panel. This limits the user's access to certain applications when the Enabler is controlling the mobile device display.

SaaS

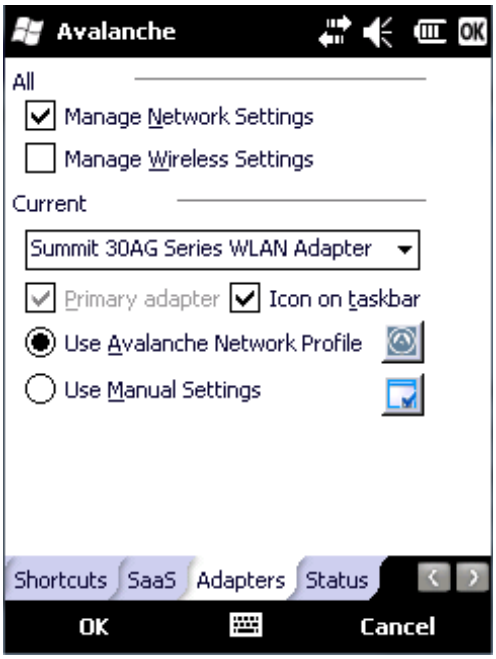


Use to configure the Enabler to connect with Avalanche on Demand. This is a Software-as-a-Service version of Avalanche. Using either of the SaaS configuration options below assumes the user has registered with Wavelink.

Setting	Function
Disable SaaS	No SaaS connection is used.
Scan Configure SaaS	Scan bar codes printed from within the Avalanche Console to configure the Enabler for the SaaS connection.
Manually Configure SaaS	Manually enter the SaaS connection information. Enter the server address on the Connection tab and the customer ID in the Company text box.

Adapters

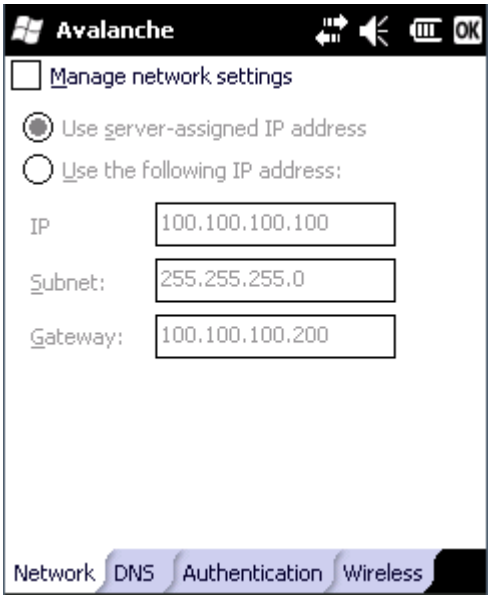
Note: Review the MX7 Tecton network settings configuration utilities and the default values before setting All Adapters to Enable in the Adapters applet..

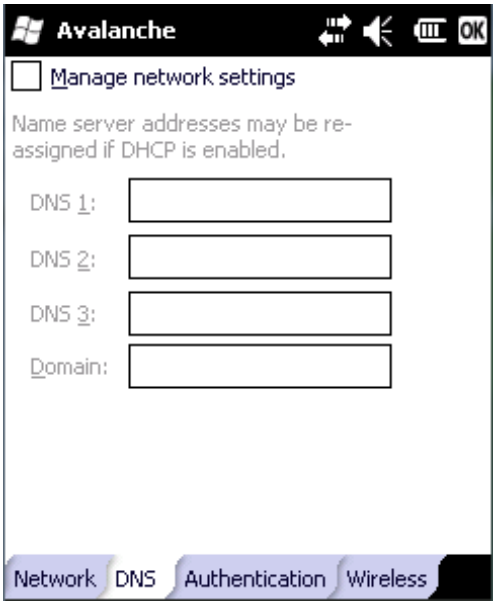


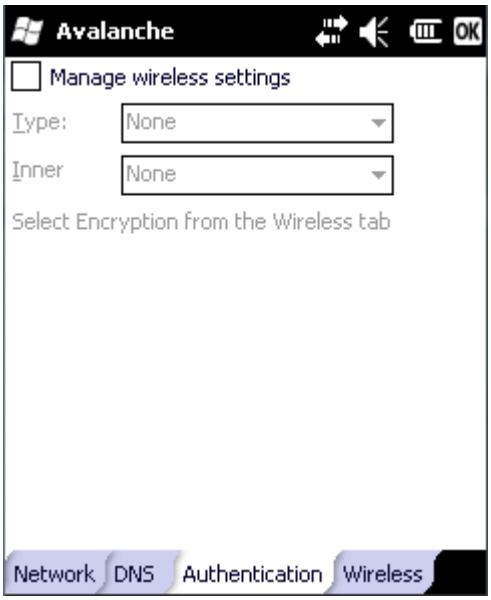
Setting	Function
Manage Network Settings	When enabled, the Enabler will control the network settings. This parameter cannot be configured from the Avalanche Mobility Center Console and is enabled by default.
Manage Wireless Settings	When enabled, the Enabler will control the wireless settings. This parameter cannot be configured from the Avalanche Mobility Center Console and is disabled by default. For Summit clients, Manage Wireless Settings should not be checked because configuration packages provide more radio configuration options.
Current Adapter	Lists all network adapters currently installed on the MX7 Tecton.
Primary Adapter	Indicates if the Enabler is to attempt to configure the primary adapter (active only if there are multiple network adapters).
Icon on taskbar	Places the Avalanche icon in the Avalanche taskbar that may, optionally, override the standard Windows taskbar.
Use Avalanche Network Profile	The Enabler will apply all network settings sent to it by the Mobile Device Server.
Avalanche Icon (varies by Enabler version)  or 	Selecting the Avalanche Icon will access the Avalanche Network Profile tab which will display current network settings.
Use Manual Settings	When enabled, the Enabler will ignore any network or wireless settings coming from the Avalanche MC Console and use only the network settings on the MX7 Tecton.
Properties Icon	Selecting the Properties icon displays the Manual Settings Properties dialog applet. From here, the user can configure Network, DNS, Authentication and Wireless parameters using the displays shown below. Note the authentication tab may not be present in all versions of the Enabler.

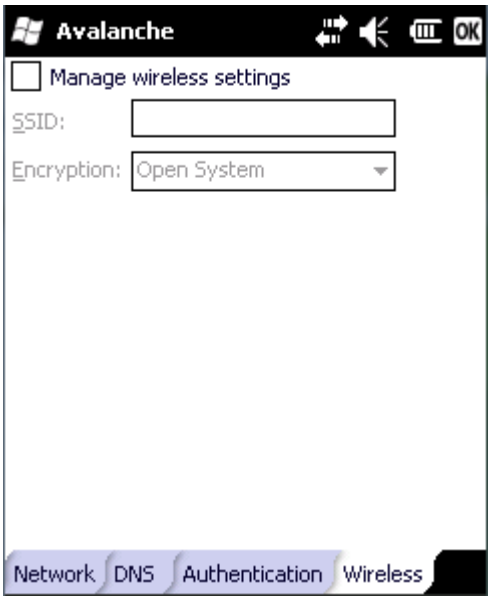
Note: A reboot may be required after enabling or disabling these options.

Manual Settings Properties









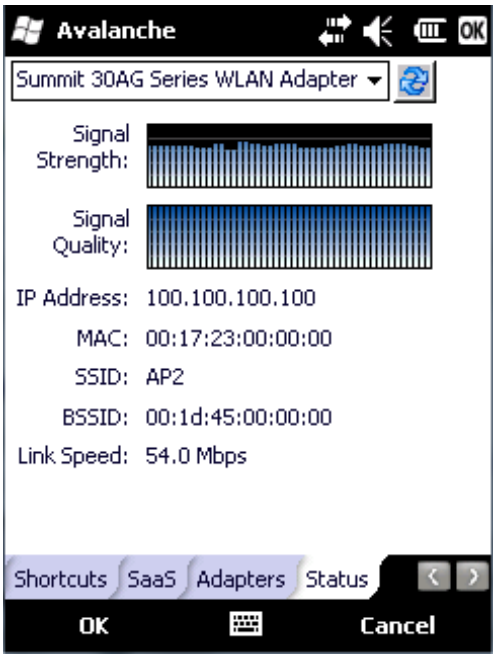
Do not enable “Manage Wireless Settings” for Summit Client devices.

Note: When you download a profile that is configured to manage network and wireless settings, the Enabler will not apply the manage network and wireless settings to the adapter unless the global Manage wireless settings and Manage network settings options are enabled on the Adapters panel. Until these options are enabled, the network and wireless settings are controlled by the third-party software associated with these settings.

Status

The Status panel displays the current status of the MX7 Tecton network adapter selected in the drop down box. Note the availability of the Windows standard Refresh button.

When the Windows Refresh button is tapped, the signal strength, signal quality and link speed are refreshed for the currently selected adapter. It also searches for new adapters and may cause a slight delay to refresh the contents of the drop-down menu.



Link speed indicates the speed at which the signal is being sent from the adapter to the MX7 Tecton. Speed is dependent on signal strength.

Exit

The Exit option is password protected. The default password is **leave**. The password is not case-sensitive.

Depending on the behavior chosen for the Shutdown setting the following screen may be displayed:

Note: The icon on the screen above may differ based on the version of the Enabler installed on the MX7 Tecton.

Change the option if desired. Tap the X button to cancel Exit. Tap the OK button to exit the Avalanche applet.

Using Remote Management

1. Configure the radio to connect to the network running the Mobile Device Server. After the MX7 Tecton is connected, proceed to step 2.
2. If it is desired to configure the radio using the Summit package, add the configured package to the Wavelink Avalanche MC Console and enable it.
3. Verify RMU.CE.CAB exists in the \System\RMU folder.
4. Double tap the MX7 Tecton enabler CAB file in the \System folder.
5. The enabler automatically launches after installation and contacts the Mobile Device Server. The Avalanche MC Console connected to that Mobile Device Server identifies the remote device and performs a sync. This downloads any available packages available for the MX7 Tecton.

Using eXpress Scan

eXpress Scan Desktop Icon

If the MX7 Tecton has an eXpress Scan icon on the desktop, eXpress Scan may be used for the initial configuration of the device.

If the eXpress Scan icon is not present on the desktop, install the Enabler. If the icon is still not present, Enabler must be updated.

If the eXpress Scan icon is present, follow these steps to configure the MX7 Tecton to connect with the wireless network and the Mobile Device Server.

Creating Bar Codes

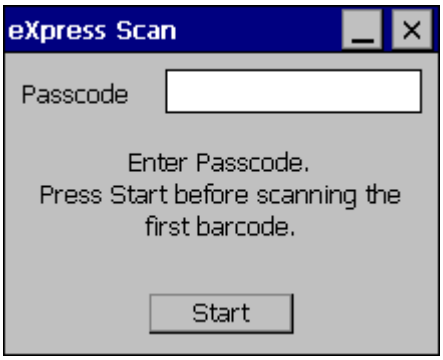
Bar codes are created with the eXpress Config utility on the desktop/laptop computer, not the mobile device. Depending on the bar code length and the number of parameters selected, eXpress Config generates one or more bar codes for device configuration. The bar codes contain configuration parameters for the wireless client and may also specify the address of the Mobile Device Server.

Bar codes should be printed at a minimum of 600 dpi.

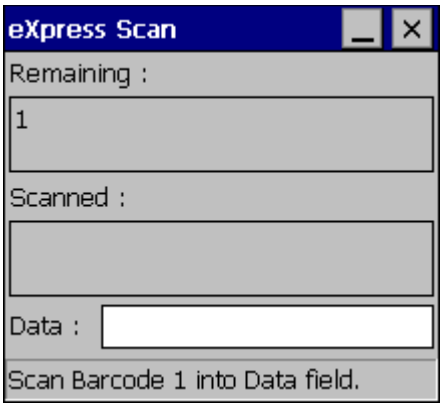
Scanning Bar Codes

Folow these instructions for each device to be configured.

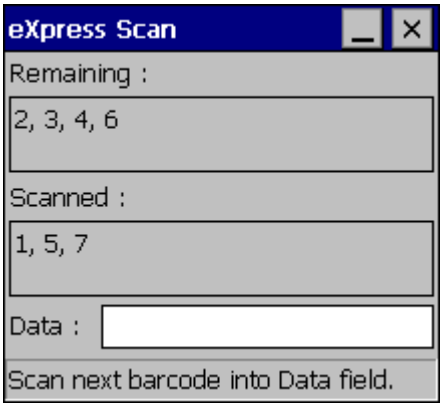
1. Start eXpress Scan on the MX7 Tecton by double tappng the eXpress Scan icon.
2. Enter the bar code passcode, if any.



3. Tap Start.
4. Bar Code 1 must be scanned first. The scanned data is displayed in the “Data” text box. The password, if any, entered above is compared to the password entered when the bar codes were created.



5. If the passwords match, the bar code data is processed and the screen is updated to reflect the number of bar codes included in the set.
6. If the passwords do not match, an error message is displayed. The current screen can be closed using the X box in the upper right corner. The password can be re-entered and Bar Code 1 scanned again.



7. The remaining bar codes may be scanned in any order. After a bar code is scanned, the bar code is removed from the “Remaining:” list and placed in the “Scanned:” list.

Process Complete

After the last bar code is scanned, the settings are automatically applied.

Once configured, the MX7 Tecton is warmbooted. After it reconnects to the wireless network and the Mobile Device Server, any software updates and additional configuration data are downloaded.

11 Wireless Network Configuration

Introduction

The Summit client device is a Summit 802.11a/b/g radio, capable of 802.11a, 802.11b and 802.11g data rates. The radio can be configured for no encryption, WEP encryption or WPA security.

Security options supported are:

- No Security (page 11-21)
- WEP (page 11-22)
- LEAP (page 11-23)
- WPA PSK (page 11-35)
- WPA/LEAP (page 11-29)
- PEAP/MSCHAP (page 11-25)
- PEAP/GTC (page 11-27)
- EAP-TLS (page 11-33)
- EAP-FAST (page 11-31)

Important Notes

⚠	It is important that all dates are correct on the MX7 Tecton and host computers when using any type of certificate. Certificates are date sensitive and when the date is not correct authentication will fail.
⚠	It may be necessary to upgrade radio software in order to use certain Summit Client Utility (SCU) features. Contact Technical Assistance (page 16-1) for details.
⚠	When using the 802.11a radio, the U-NII 1 band is the preferred band for indoor operation. For regulatory domains in which the U-NII 3 band is allowed, the following channels are supported: 149, 153, 157 and 161. The AP must be configured accordingly.

After making any changes to the wireless configuration, perform a Suspend/Resume on the MX7 Tecton.

Summit Client Utility

Note: When making changes to profile or global parameters, tap the power key to place the MX7 Tecton in Suspend. When the MX7 Tecton resumes from suspend the parameters are applied. The MX7 Tecton can be resumed by tapping the power key or the touch screen or by pressing any key.

Select the Summit Client Utility using the Start button or tap the Summit Tray Icon (if present).

The Main (page 11-5)provides information, admin login and active profile selection.

Profile specific parameters are found on the Profile (page 11-8). The parameters on this tab can be set to unique values for each profile.

The Status (page 11-11) contains information on the current connection.

The Diags (page 11-12) provides utilities to troubleshoot the radio.

Global parameters are found on theGlobal (page 11-13). The values for these parameters apply to all profiles.

Help

Help is available by tapping the **?** icon in the title bar on most Summit Client Utility (SCU) screens.

Help may also be accessed by selecting **Start > Help** and tapping the Summit Client Utility link. The SCU does not have to be open to view the help information using this option.

Summit Tray Icon

The Summit tray icon provides access to the SCU and is a visual indicator of radio status.

The Summit tray icon is displayed when:

- The Summit radio is installed and active
- The Windows Zero Config utility is not active
- The Tray Icon setting is On

Tap the icon to launch the SCU. Use the tray icon to view the radio status:

	The radio is not currently associated or authenticated to an Access Point
	The signal strength for the currently associated/authenticated Access Point is less than -90 dBm
	The signal strength for the currently associated/authenticated Access Point is -71 dBm to -90 dBm
	The signal strength for the currently associated/authenticated Access Point is -51 dBm to -70 dBm
	The signal strength for the currently associated/authenticated Access Point is greater than -50 dBm

Using Windows Mobile Wireless Manager

Using the Summit Client Utility to manage wireless connectivity is recommended. However, if desired, Windows Mobile includes the Wireless Manager utility to manage wireless network connections in place of the Summit Client Utility.

To use the Windows Mobile Wireless Manager, first open the Summit Client Utility.

1. Select **ThirdPartyConfig** in the Active Profile drop down box on the Main (page 11-5).
2. A message appears that a Power Cycle is required to make settings activate properly.
3. Tap **OK**.
4. Open the Registry (page 5-45) panel and tap Warmboot.

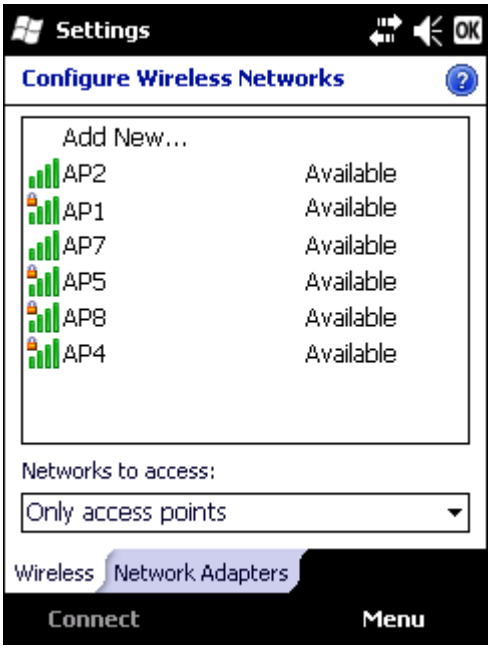
Access the Wireless Manager utility by tapping the radio icon at the top of the screen or tapping **Start > Settings > Connections > Wi-Fi**.

If the Wi-Fi icon is not present in the Connections panel, return to the Summit Client Utility and select **ThirdPartyConfig**.

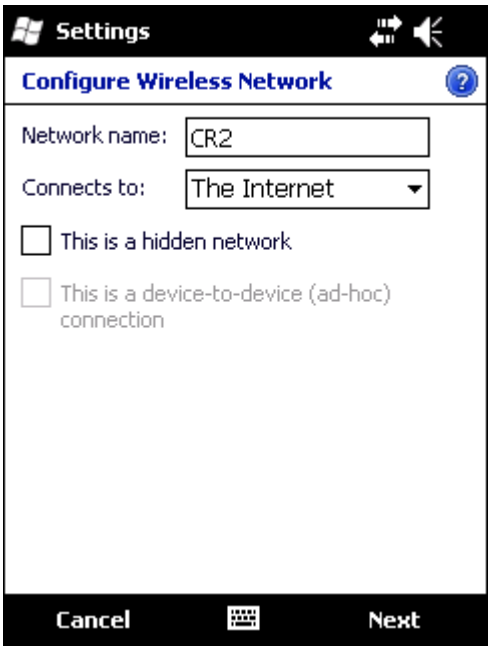
Refer to the Windows Mobile help screens or online documentation for configuring wireless security using the Windows Mobile Wireless Manager.

Create a New Network Connection

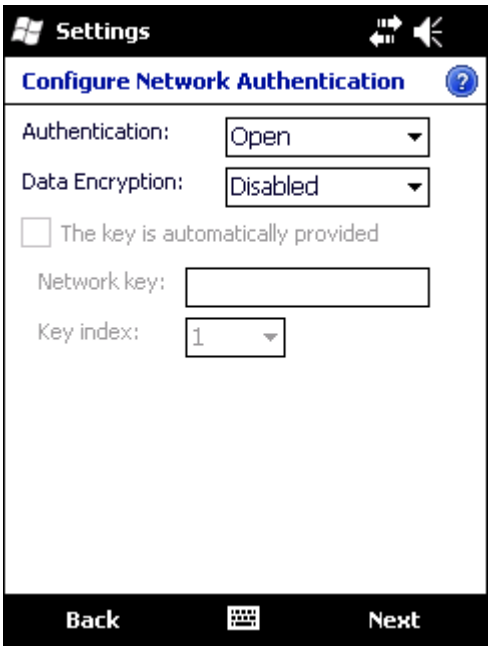
1. Tap on the Wi-Fi icon. A list of available networks is displayed.



2. If the desired network is not displayed, tap **Add New**. If the desired network is displayed in the list, tap the network name.



3. Enter the SSID of the desired network in the **Network name** text box. Be sure to check the *This is a hidden network* check box for a non-broadcast SSID.
4. In the **Connects to** box, select **The Internet** if the MX7 Tecton connects directly to the Internet, select Work if the MX7 Tecton connects to a network (even if the network provides an Internet connection).
5. Tap **Next.**



Edit a Network Connection

Double tap the network name to edit the configuration or tap the network name and tap **Connect** to connect to the network.

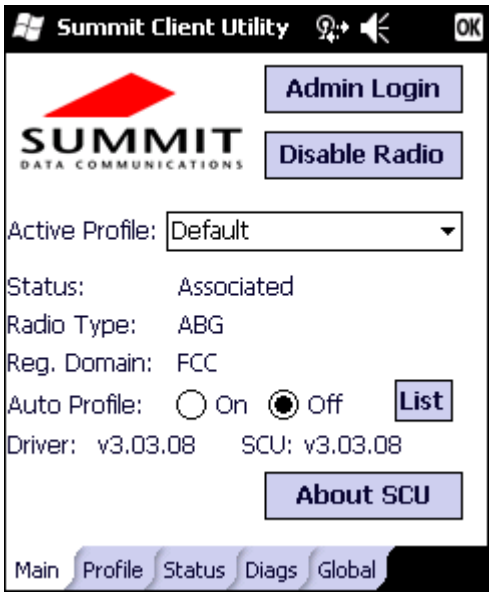
Network configuration screens are the same as displayed in the previous section.

Switch Control to SCU

1. To switch back to SCU control, select any other profile except **ThirdPartyConfig** in the SCU Active Config drop down list on the Main tab.
2. A message appears that a Power Cycle is required to make settings activate properly.
3. Tap **OK**.
4. Open the Registry panel and tap Warmboot. Radio control is passed to the Summit Client Utility.

Main

Setting	Default
Admin Login	SUMMIT
Radio	Enabled
Active Config/Profile	Default
Regulatory Domain	Varies by location



The Main tab displays information about the wireless client device including:

- SCU (Summit Client Utility) version
- Driver version
- Radio Type (ABG is an 802.11 a/b/g radio).
- Regulatory Domain is preset to either Worldwide or a location specific domain (FCC, ETSI, KCC or TELEC).
- Copyright Information can be accessed by tapping the About SCU button
- Active Config profile / Active Profile name
- Status of the client (Down, Associated, Authenticated, etc.).

The **Active Profile** can be switched without logging in to Admin mode. Selecting a different profile from the drop down list does not require logging in to Administrator mode. The profile must already exist. Perform a Suspend/Resume function when changing profiles. Profiles can be created or edited after the Admin login password has been entered and accepted.

When the profile named *ThirdPartyConfig* is chosen as the active profile, the Summit Client Utility passes control to Wireless Manager for configuration of all client and security settings for the network module.

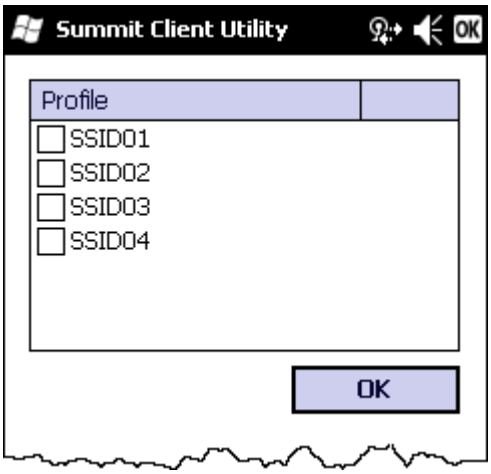
The **Disable Radio** button can be used to disable the network card. Once disabled, the button label changes to *Enable Radio*. By default the radio is enabled.

The **Admin Login** button provides access to editing wireless parameters. Profile and Global may only be edited after entering the Admin Login password. The password is case-sensitive.

Once logged in, the button label changes to *Admin Logout.* To logout, either tap the **Admin Logout** button or exit the SCU without tapping the **Admin Logout** button.

Auto Profile

Auto Profile allows the user to configure a list of profiles that the SCU can search when a radio connection is lost. After using the Profile tab to create any desired profiles, return to the Main tab. To specify which profiles are to be included in Auto Profile, tap the **List** button.



The Auto Profile selection screen displays all currently configured profiles. Tap on the check box for any profiles that are to be included in Auto Profile selection then tap ok to save.

To enable Auto Profile, tap the On button on the Main tab.

When Auto Profile is On, if the radio goes out of range from the currently selected profile, the radio then begins to attempt to connect to the profiles listed under Auto Profile.

The search continues until:

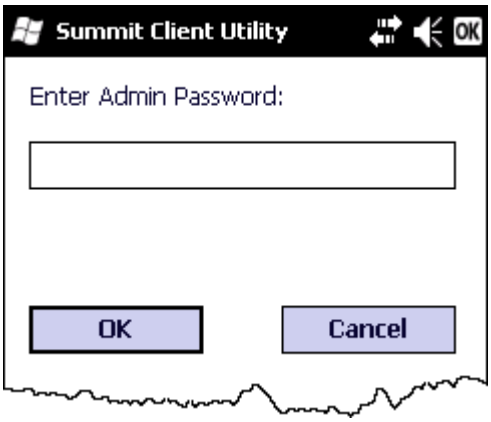
- the SCU connects to and, if necessary, authenticates with, one of the specified profiles or
- the Off button is tapped to turn off Auto Profile.

Note: Do not include any profiles with an Ad Hoc Radio Mode in this listing.

Admin Login

To login to Administrator mode, tap the **Admin Login** button.

Once logged in, the button label changes to Admin Logout. The admin is automatically logged out when the SCU is exited. The Admin can either tap the **Admin Logout** button, or the **OK** button to logout.



Enter the Admin password (the default password is SUMMIT and is case sensitive) and tap OK. If the password is incorrect, an error message is displayed.

The Administrator default password can be changed on the Global (page 11-13).

The end-user can:

- Turn the radio on or off on the Main tab.
- Select an active Profile on the Main tab.
- View the current parameter settings for the profiles on the Profile (page 11-8).
- View the global parameter settings on the Global (page 11-13).
- View the current connection details on the Status (page 11-11).
- View radio status, software versions and regulatory domain on the Main (page 11-5).
- Access additional troubleshooting features on the Diags (page 11-12).

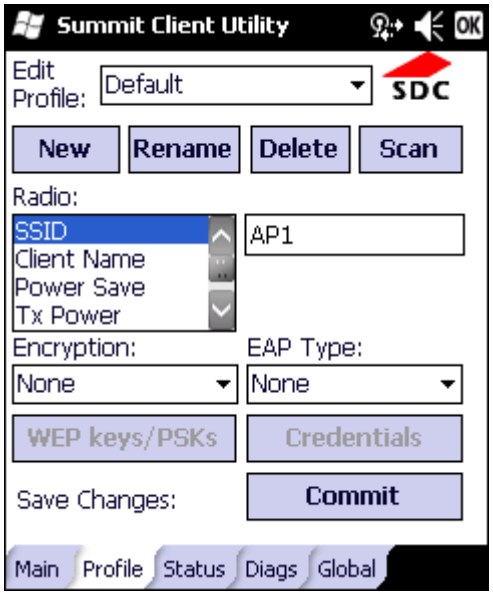
After Admin Login, the end-user can also:

- Create, edit, rename and delete profiles on the Profile (page 11-8).
- Edit global parameters on the Global (page 11-13).
- Enable/disable the Summit tray icon in the taskbar.

Profile

Note: Tap the Commit button to save changes before leaving this panel or the SCU. If the panel is exited before tapping the Commit button, changes are not saved!

Setting	Default
Profile	Default
SSID	Blank
Client Name	Blank
Power Save	Fast
Tx Power	Maximum
Bit Rate	Auto
Radio Mode	See Profile Parameters (page 11-10) for default
Auth Type	Open
EAP Type	None
Encryption	None



When logged in as an Admin, see Admin Login (page 11-6), use the Profile tab to manage profiles. When not logged in as an Admin, the parameters can be viewed, and cannot be changed. The buttons on this tab are dimmed if the user is not logged in as Admin. The Profile tab was previously labeled Config.

Note: The settings for Auth Type, EAP Type and Encryption depend on the security type chosen.

Buttons

New Button

Creates a new profile with the default settings (see Profile Parameters) and prompts for a unique name. If the name is not unique, an error message is displayed and the new profile is not created.

Rename Button

Assigns a new, unique name. If the new name is not unique, an error message is displayed and the profile is not renamed.

Delete Button

Deletes the profile. The current active profile cannot be deleted and an error message is displayed if a delete is attempted.

WEP Keys / PSK Keys Button

Allows entry of WEP keys or pass phrase as required by the type of encryption.

Credentials Button

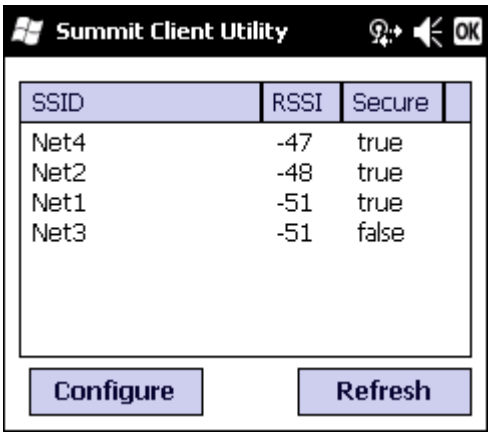
Allows entry of a user name and password, certificate names, and other information required to authenticate with the access point. The information required depends on the EAP type.

Commit Button

Saves the profile settings made on this screen. Settings are saved in the profile.

Scan Button

Opens a window that lists access points that are broadcasting their SSIDs. Tap the Refresh button to view an updated list of APs. Each AP's SSID, its received signal strength indication (RSSI) and whether or not data encryption is in use (true or false). Sort the list by tapping on the column headers. If you are logged in as an Admin, tap an SSID in the list and tap the Configure button, you return to the Profile window to recreate a profile for that SSID, with the profile name being the same as the SSID (or the SSID with a suffix such as "_1" if a profile with the SSID as its name exists already). If the scan finds more than one AP with the same SSID, the list displays the AP with the strongest RSSI and the least security.

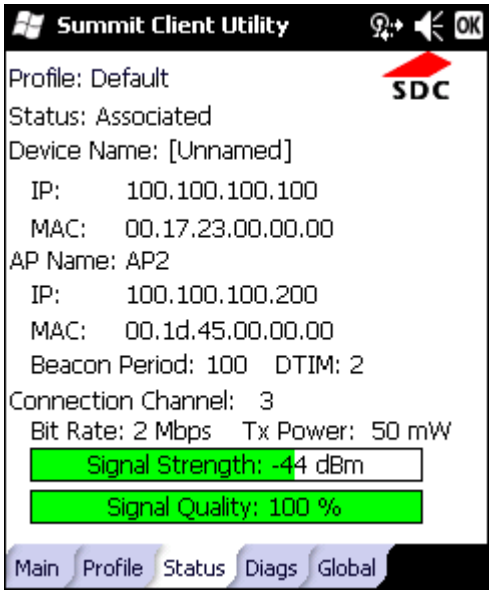


Note: Unsaved Changes – The SCU will display a reminder if the Commit button is not tapped before an attempt is made to close or browse away from this tab.

Profile Parameters

Parameter	Default	Explanation
Edit Profile	Default	A string of 1 to 32 alphanumeric characters, establishes the name of the Profile. Options are Default or ThirdPartyConfig.
SSID	Blank	A string of up to 32 alphanumeric characters. Establishes the Service Set Identifier (SSID) of the WLAN to which the client connects.
Client Name	Blank	A string of up to 16 characters. The client name is assigned to the network card and the device using the network card. The client name may be passed to networking wireless devices, e.g., Access Points.
Power Save	Fast	Power save mode is On. Options are: Constantly Awake Mode (CAM) power save off, Maximum (power saving mode) and Fast (power saving mode). When using power management, use FAST for best throughput results.
Tx Power	Maximum	Maximum setting regulates Tx power to the Max power setting for the current regulatory domain. Options are: Maximum, 50mW, 30mW, 20mW, 10mW, 5mW, or 1mW.
Bit Rate	Auto	Setting the rate to Auto will allow the Access Point to automatically negotiate the bit rate with the client device. This parameter cannot be changed.
Auth Type	Open	802.11 authentication type used when associating with the Access Point. Options are: Open, LEAP, or Shared key.
EAP Type	None	Extensible Authentication Protocol (EAP) type used for 802.1x authentication to the Access Point. Options are: None, LEAP, EAP-FAST, PEAP-MSCHAP, PEAP-GTC, PEAP-TLS, EAP-TTLS, or EAP-TLS. *Note: EAP Type chosen determines whether the Credentials button is active and also determines the available entries in the Credentials pop-up window.*
Encryption	None	Type of encryption to be used to protect transmitted data. Available options may vary by SCU version. Options are: None, WEP (or Manual WEP), WEP EAP (or Auto WEP), WPA PSK, WPA TKIP, WPA CCKM, WPA2 PSK, WPA2 AES, or WPA2 CCKM. CKIP is not supported in the MX7 Tecton. *Note: The Encryption type chosen determines if the WEP Keys / PSK Keys button is active and also determines the available entries in the WEP or PSK pop-up window.*
Radio Mode	BGA Rates Full	Specify 802.11a, 802.11b and/or 802.11g rates when communicating with the AP. The options displayed for this parameter depend on the type of radio installed in the MX7 Tecton. Options: • B rates only (1, 2, 5.5 and 11 Mbps) • BG Rates Full (All B and G rates • G rates only (6, 9, 12, 18, 24, 36, 48 and 54 Mbps • A rates only (6, 9, 12, 18, 24, 36, 48 and 54 Mbps • ABG Rates Full (All A rates and all B and G rates with A rates preferred • BGA Rates Full (All B and G rates and all A rates with B and G rates preferred • Ad Hoc (when connecting to another client device instead of an AP) Default: BGA Rates Full (for 802.11a/b/g radio) *Note: It is important the Radio Mode parameter correspond to the AP to which the device is to connect. For example, if this parameter is set to G rates only, the MX7 Tecton may only connect to APs set for G rates and not those set for B and G rates.*

Status



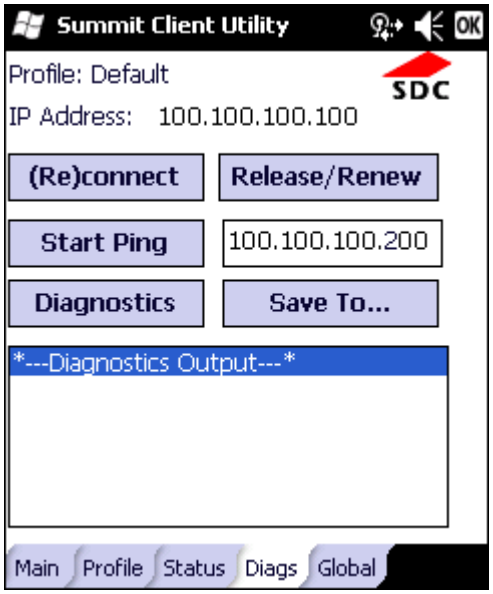
This screen provides information on the radio:

- The profile in use.
- The status of the radio card (down, associated, authenticated, etc.)
- Client information including device name, IP address and MAC address.
- Information about the Access Point (AP) maintaining the connection to the network including AP name, IP address and MAC address.
- Channel currently being used for wireless traffic.
- Bit rate in Mbit.
- Current transmit power in mW.
- Beacon period – the time between AP beacons in kilo-microseconds. (one kilo-microsecond = 1,024 microseconds).
- DTIM interval – A multiple of the beacon period that specifies how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power saving devices a packet is waiting for them. For example, if DTIM = 3, then every third beacon contains a DTIM.
- Signal strength (RSSI) displayed in dBm and graphically.
- Signal quality, a measure of the clarity of the signal displayed in percentage and graphically.

There are no user entries on this screen.

Note: After completing radio configuration, it is a good idea to review this screen to verify the radio has associated (no encryption, WEP) or authenticated (LEAP, any WPA), as indicated above.

Diags



The Diags screen can be used for troubleshooting network traffic and radio connectivity issues.

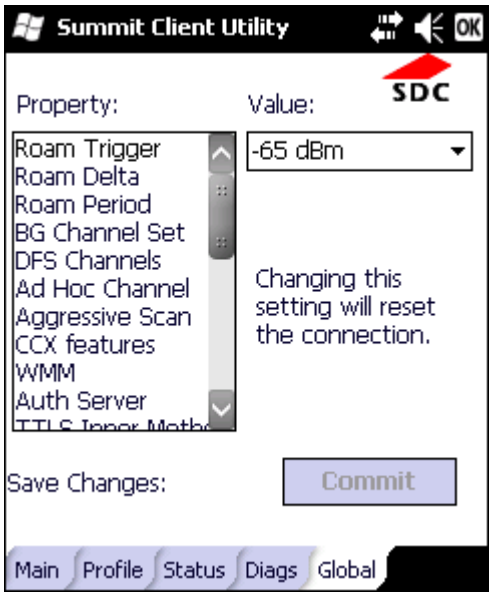
- **(Re)connect** – Use this button to apply (or reapply) the current profile and attempt to associate or authenticate to the wireless LAN. All activity is logged in the Diagnostic Output box on the lower part of the screen.
- **Release/Renew** – Obtain a new IP address through release and renew. All activity is logged in the Diagnostic Output box. If a fixed IP address has been assigned to the radio, this is also noted in the Diagnostic Output box. Note that the current IP address is displayed above this button.
- **Start Ping** – Start a continuous ping to the IP address specified in the text box to the right of this button. Once the button is tapped, the ping begins and the button label changes to **Stop Ping**. Tapping the button ends the ping. The ping also ends when any other button on this screen is tapped or the user browses away from the Diags tab. The results of the ping are displayed in the Diagnostic Output box.
- **Diagnostics** – Also attempts to (re)connect to the wireless LAN. However, this option provides more data in the Diagnostic Output box than the (Re)connect option. This data dump includes radio state, profile settings, global settings, and a list of broadcast SSID APs.
- **Save To…** – Use this to save the results of the diagnostics to a text file. Use the explorer window to specify the name and location for the diagnostic file. The text file can viewed using an application such as WordPad.

Global

The parameters on this panel can only be changed when an Admin is logged in with a password. The current values for the parameters can be viewed by the general user without requiring a password.

Note: Tap the Commit button to save changes. If the panel is exited before tapping the Commit button, changes are not saved!

Setting	**Default**
Roam Trigger	-65 dBm
Roam Delta	5 dBm
Roam Period	10 sec.
BG Channel Set	Full
DFS Channels	Off
DFS Scan Time	120 ms.
Ad Hoc Channel	1
Aggressive Scan	On
CCX Features	Optimized
WMM	Off
Auth Server	Type 1
TTLS Inner Method	Auto-EAP
PMK Caching	Standard
WAPI	Off (dimmed)
TX Diversity	On
RX Diversity	On Start on Main
Frag Threshold	2346
RTS Threshold	2347
LED	Off
Tray Icon	On
Hide Passwords	On
Admin Password	SUMMIT (or blank)
Auth Timeout	8 seconds
Certs Path	System
Ping Payload	32 bytes
Ping Timeout	5000 ms
Ping Delay ms	1000 ms



Custom Parameter Option

The parameter Custom option is not supported. The parameter value is displayed as “Custom” when the operating system registry has been edited to set the Summit parameter to a value that is not available from the parameter’s drop down list. Selecting Custom from the drop down list has no effect. Selecting any other value from the drop down list will overwrite the “custom” value in the registry.

Global Parameters

Parameter	Default	Function
Roam Trigger	-65 dBm	If signal strength is less than this trigger value, the client looks for a different Access Point with a stronger signal. Options are: -50 dBm, -55, -60, -65, -70, -75, -80, -85, -90 dBm or Custom Parameter Option (page 11-14).
Roam Delta	5 dBm	The amount by which a different Access Point signal strength must exceed the current Access Point signal strength before roaming to the different Access Point is attempted. Options are: 5 dBm, 10, 15, 20, 25, 30, 35 dBm or Custom Parameter Option (page 11-14).
Roam Period	10 sec.	The amount of time, after association or a roam scan with no roam, that the radio collects Received Signal Strength Indication (RSSI) scan data before a roaming decision is made. Options are: 5 sec, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60 seconds or Custom Parameter Option (page 11-14).
BG Channel Set	Full	Defines the 2.4GHz channels to be scanned for an AP when the radio is contemplating roaming. By specifying the channels to search, roaming time may be reduced over scanning all channels. Options are: • Full (all channels) • 1,6,11 (the most commonly used channels) • 1,7,13 (for ETSI and TELEC radios only) • Custom Parameter Option (page 11-14).
DFS Channels	Off	Support for 5GHZ 802.11a channels where support for DFS is required. Options are: On, Off. *Note: Not supported (always off) in some releases.*
DFS Scan Time	120 ms.	The amount of time the radio will passively scan each DFS channel to see if it will receive a beacon. Recommended value is 1.5 times that of the AP's beacon period.

Parameter	Default	Function
Ad Hoc Channel	1	Use this parameter when the Radio Mode profile parameter is set to Ad Hoc. Specifies the channel to be used for an Ad Hoc connection to another client device. If a channel is selected that is not supported by the by the radio, the default value is used. Options are: • 1 through 14 (the 2.4GHz channels) • 36, 40, 44, 48 (the UNII-1 channels)
Aggressive Scan	On	When set to On and the current connection to an AP weakens, the radio aggressively scans for available APs. Aggressive scanning works with standard scanning (set through Roam Trigger, Roam Delta and Roam Period). Aggressive scanning should be set to On unless there is significant co-channel interference due to overlapping APs on the same channel. Options are: On, Off
CCX Features	Optimized	Use of Cisco Compatible Extensions (CCX) radio management and AP specified maximum transmit power features. This parameter cannot be changed.
WMM	Off	Use of Wi-Fi Multimedia extensions. Options are: On, Off Default value cannot be changed.
Auth Server	Type 1	Specifies the type of authentication server. Options are: Type 1 (ACS server) and Type 2 (non-ACS server)
TTLS Inner Method	Auto-EAP	Authentication method used within the secure tunnel created by EAP-TTLS. Options are: AUTO-EAP (Any available EAP method), MSCHAPV2, MSCHAP, PAP, CHAP, EAP-MSCHAPV2
PMK Caching	Standard	Type of Pairwise Master Key (PMK) caching to use when WPA2 is in use. PMK caching is designed to speed up roaming between APs by allowing the client and the AP to cache the results of 802.1X authentications, eliminating the need to communicate with the ACS server. Standard PMK is used when there are no controllers. The reauthentication information is cached on the original AP. The client and the AP use the cached information to perform the four-way handshake to exchange keys. Opportunistic PMK (OPMK) is used when there are controllers. The reauthentication information cached on the controllers. The client and the controller behind the AP use the cached information to perform the four-way handshake to exchange keys. If the selected PMK caching method is not supported by the network infrastructure, every roam requires full 802.11X authentication, including interaction with the ACS server. If the active profile is using WPA2 CCKM, the global PMK Caching setting is ignored and the client attempts to use CCKM. Options are: Standard, OPMK *Note: This change does not take effect until after a Suspend/Resume cycle.*
WAPI	Off	Default is Off and dimmed (cannot be changed)
TX Diversity	On	How to handle antenna diversity when transmitting packets to the Access Point. Options are: Main only, and On.
RX Diversity	On-Start on Main	How to handle antenna diversity when receiving packets from the Access Point. Options are: On-Start on Main and Main only.
Frag Thresh	2346	If the packet size (in bytes) exceeds the specified number of bytes set in the fragment threshold, the packet is fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of wireless interference. This parameter cannot be changed.
RTS Thresh	2347	If the packet size exceeds the specified number of bytes set in the Request to Send (RTS) threshold, an RTS is sent before sending the packet. A low RTS threshold setting can be useful in areas where many client devices are associating with the Access Point. This parameter cannot be changed.

Parameter	Default	Function
LED	Off	The LED on the wireless card is not visible to the user when the wireless card is installed in a sealed mobile device. Options are: On, Off. This parameter cannot be changed.
Tray Icon	On	Determines if the Summit icon is displayed in the System tray. Options are: On, Off
Hide Password	On	When On, the Summit Config Utility masks passwords (characters on the screen are displayed as an *) as they are typed and when they are viewed. When Off, password characters are not masked. Options are: On, Off.
Admin Password	SUMMIT (or Blank)	A string of up to 64 alphanumeric characters that must be entered when the Admin Login button is tapped. If Hide Password is On, the password is masked when typed in the Admin Password Entry dialog box. The password is case sensitive. This value is masked when the Admin is logged out. Options are: none.
Auth Timeout	8 seconds	Specifies the number of seconds the Summit software waits for an EAP authentication request to succeed or fail. If the authentication credentials are stored in the active profile and the authentication times out, the association fails. No error message or prompting for corrected credentials is displayed. If the authentication credentials are not stored in the active profile and the authentication times out, the user is again prompted to enter the credentials. Options are: An integer from 3 to 60.
Certs Path	System	A valid directory path, of up to 64 characters, where WPA Certificate Authority and User Certificates are stored on the mobile device when not using the Windows certificates store. Make sure the Windows folder path currently exists before assigning the path in this parameter. See Certificates for instructions on obtaining CA and User Certificates. This value is masked when the Admin is logged out. Options are: none. For example, when the valid certificate is stored as My Computer/System/MYCERTIFICATE.CER, enter System in the Certs Path text box as the Windows folder path.
Ping Payload	32 bytes	Maximum amount of data to be transmitted on a ping. Options are: 32 bytes, 64, 128, 256, 512, or 1024 bytes.
Ping Timeout ms	5000	The amount of time, in milliseconds, that a device will be continuously pinged. The Stop Ping button can be tapped to end the ping process ahead of the ping timeout. Options are: Any number between 0 and 30000 ms.
Ping Delay ms	1000	The amount of time, in milliseconds, between each ping after a Start Ping button tap. Options are: Any number between 0 and 30000 ms.

Note: Tap the Commit button to save changes. If this panel is closed before tapping the Commit button, changes are not saved!

Sign-On vs. Stored Credentials

When using wireless security that requires a user name and password to be entered, the Summit Client Utility offers the following choices:

- The Username and Password may be entered on the Credentials screen. If this method is selected, anyone using the device can access the network.
- The Username and Password are left blank on the Credentials screen. When the device attempts to connect to the network, a sign on screen is displayed. The user must enter the Username and Password at that time to authenticate.

Using Stored Credentials

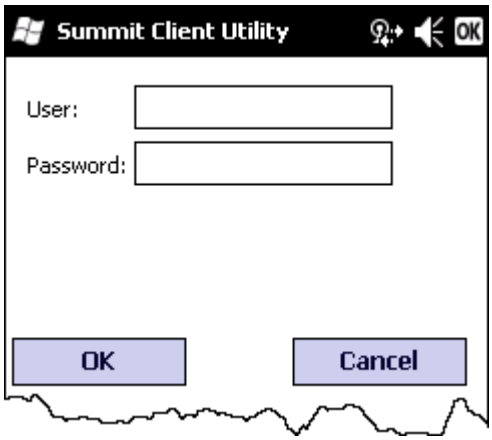
1. After completing the other entries in the profile, tap on the Credentials button.
2. Enter the Username and Password on the Credentials screen and tap the OK button.
3. Tap the Commit button.
4. For LEAP and WPA/LEAP, configuration is complete.
5. For PEAP-MSCHAP and PEAP-GTC, importing the CA certificate into the Windows certificate store is optional.
6. For EAP-TLS, import the CA certificate into the Windows certificate store. Also import the User Certificate into the Windows certificate store.
7. Access the Credentials screen again. Make sure the Validate server and Use MS store checkboxes are checked.
8. The default is to use the entire certificate store for the CA certificate. Alternatively, use the Browse button next to the CA Cert (CA Certificate Filename) on the Credentials screen to select an individual certificate.
9. For EAP-TLS, also enter the User Cert (User Certificate filename) on the credentials screen by using the Browse button.
10. If using EAP FAST and manual PAC provisioning, input the PAC filename and password..
11. Tap the OK button then the Commit button.
12. If changes are made to the stored credentials, tap Commit to save those changes before making any additional changes to the profile or global parameters.
13. Verify the device is authenticated by reviewing the Status tab. When the device is property configured, the Status tab indicates the device is Authenticated and the method used.

Note: See Configuring Profiles (page 11-21) for more details.

Note: If invalid credentials are entered into the stored credentials, the authentication will fail. No error message is displayed. The user may or may not be prompted to enter valid credentials.

Using a Sign On Screen

1. After completing the other entries in the profile, tap on the Credentials button. Leave the Username and Password blank. No entries are necessary on the Credentials screen for LEAP or LEAP/WPA.
2. For PEAP-MSCHAP and PEAP-GTC, importing the CA certificate into the Windows certificate store is optional.
3. For EAP-TLS, import the CA certificate into the Windows certificate store. Also import the User Certificate into the Windows certificate store.
4. Access the Credentials screen again. Make sure the Validate server and Use MS store checkboxes are checked.
5. The default is to use the entire certificate store for the CA certificate. Alternatively, use the Browse button next to the CA Cert (CA Certificate Filename) on the Credentials screen to select an individual certificate.
6. For EAP-TLS, also enter the User Cert (User Certificate filename) on the credentials screen by using the Browse button.
7. Tap the OK button then the Commit button.
8. When the device attempts to connect to the network, a sign-on screen is displayed.
9. Enter the Username and Password. Tap the OK button.



10. Verify the device is authenticated by reviewing the Status tab. When the device is property configured, the Status (page 11-11) indicates the device is Authenticated and the method used.

11. The sign-on screen is displayed after a reboot.

Note: See Configuring Profiles (page 11-21) for more details.

If a user enters invalid credentials and clicks OK, the device associates but does not authenticate. The user is again prompted to enter credentials.

If the user clicks the Cancel button, the device does not associate. The user is not prompted again for credentials until:

- the device is rebooted,
- the radio is disabled then enabled,
- the Reconnect button on the Diags Tab is tapped or
- the profile is modified and the Commit button is tapped.

Windows Certificate Store vs. Certs Path

Note: It is important that all dates are correct on the MX7 Tecton and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

User Certificates

EAP-TLS authentication requires a user certificate. The user certificate must be stored in the Windows certificate store.

- To generate the user certificate, see Generating a User Certificate (page 11-39).
- To import the user certificate into the Windows certificate store, see Installing a User Certificate (page 11-43).
- A Root CA certificate is also needed. Refer to the section below.

Root CA Certificates

Root CA certificates are required for EAP/TLS, PEAP/GTC and PEAP/MSCHAP. Two options are offered for storing these certificates:

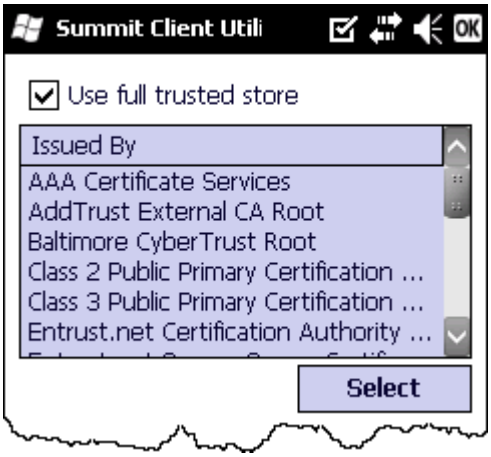
- Imported into the Windows certificate store.
- Copied into the Certs Path directory.

Using the Certs Path

1. See Generating a Root CA Certificate (page 11-36) and follow the instructions to download the Root Certificate to a PC.
2. Copy the certificate to specified directory on the mobile device. The default location for Certs Path is \System. A different location may be specified by using the Certs Path global variable. Note the location chosen for certificate storage should persist after a reboot.
3. When completing the Credentials screen for the desired authentication, do not check the Use MS store check box after tapping the Validate server check box.
4. Enter the certificate name in the CA Cert textbox.
5. Tap OK to exit the Credentials screen and then Commit to save the profile changes.

Using the Windows Certificate Store

1. See Generating a Root CA Certificate (page 11-36) and follow the instructions to download the Root Certificate to a PC.
2. To import the certificate into the Windows store, see Installing a Root CA Certificate (page 11-39).
3. When completing the Credentials screen for the desired authentication, be sure to check the Use MS store check box after tapping the Validate server check box.
4. The default is to use all certificates in the store. If this is OK, skip to the last step.
5. Otherwise, to select a specific certificate tap on the Browse (…) button.



6. Uncheck the Use full trusted store check box.
7. Select the desired certificate and tap the Select button to return the selected certificate to the CA Cert textbox.
8. Tap OK to exit the Credentials screen and then Commit to save the profile changes.

Configuring Profiles

Use the instructions in this section to complete the entries on the Profile tab according to the type of wireless security used by your network. The instructions that follow are the minimum required to successfully connect to a network. Your system may require more parameters than are listed in these instructions.See your system administrator for complete information about your network and its wireless security requirements.

To begin the configuration process:

1. On the Main Tab, tap the Admin Login button and enter the password.
2. Edit the default profile with the parameters for your network. Select the Default profile from the pull down menu.
3. Make any desired parameter changes as described in the applicable following section determined by network security type and tap the Commit button to save the changes.

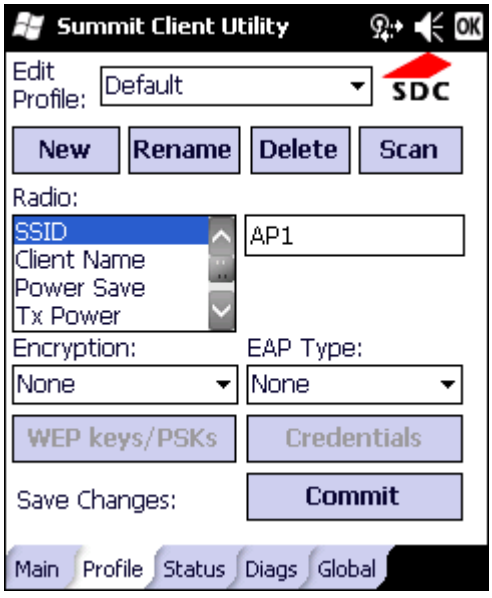
IMPORTANT – Remember to tap the Commit button after making changes to ensure the changes are saved. Many versions of the SCU display a reminder if the Commit button is not tapped before an attempt is made to close or browse away from the tab in focus if there are unsaved changes.

If changes are made to the stored credentials, tap Commit to save those changes first before making any additional changes.

No Security

To connect to a wireless network with no security, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile.
2. Set EAP Type to None.
3. Set Encryption to None.
4. Set Auth Type to Open.

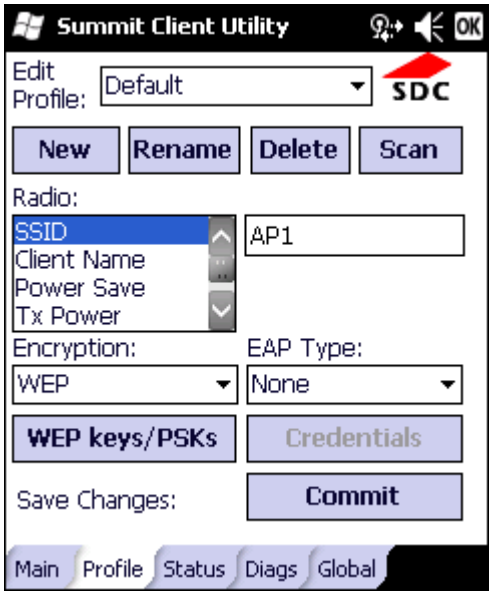


5. Once configured, tap the Commit button.
6. Ensure the correct Active Profile is selected on the Main Tab and perform a Suspend/Resume. The SCU Main tab shows the device is associated after the radio connects to the network.

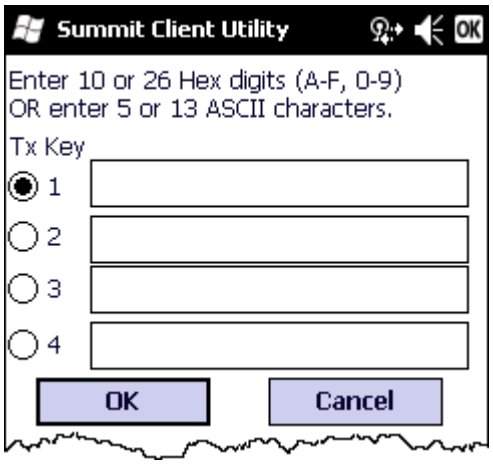
WEP

To connect using WEP, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile.
2. Set EAP Type to None.
3. Set Encryption to WEP or Manual WEP (depending on SCU version).
4. Set Auth Type to Open.



5. Tap the WEP keys/PSKs button.



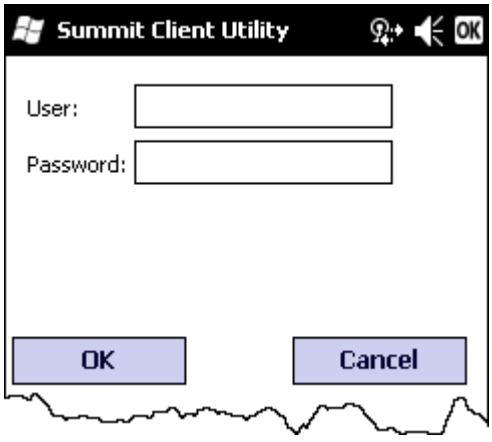
6. Valid keys are 10 hexadecimal or 5 ASCII characters (for 40-bit encryption) or 26 hexadecimal or 13 ASCII characters (for 128-bit encryption). Enter the key(s) and tap OK.
7. Once configured, tap the Commit button.
8. Ensure the correct Active Profile is selected on the Main Tab and perform a Suspend/Resume. The SCU Main tab shows the device is associated after the radio connects to the network.

LEAP

To use LEAP (without WPA), make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile.
2. Set EAP Type to LEAP.
3. Set Encryption to WEP EAP or Auto WEP (depending on SCU version).
4. Set Auth Type as follows:
   - If the Cisco/CCX certified AP is configured for open authentication, set the Auth Type radio parameter to Open.
   - If the AP is configured to use shared key or passphrase, set the Auth Type radio parameter to Shared.
   - If the AP is configured for network EAP only, set the Auth Type radio parameter to LEAP.

5. See Sign-On vs. Stored Credentials (page 11-17) for information on entering credentials.
6. To use Stored Credentials, tap on the Credentials button. No entries are necessary for Sign-On Credentials as the user will be prompted for the Username and Password when connecting to the network.



7. Enter the Domain\Username (if the Domain is required), otherwise enter the Username.
8. Enter the password.

9. Tap OK then tap Commit.

10. Ensure the correct Active Profile is selected on the Main Tab and perform a Suspend/Resume. The SCU Main tab shows the device is associated after the radio connects to the network.

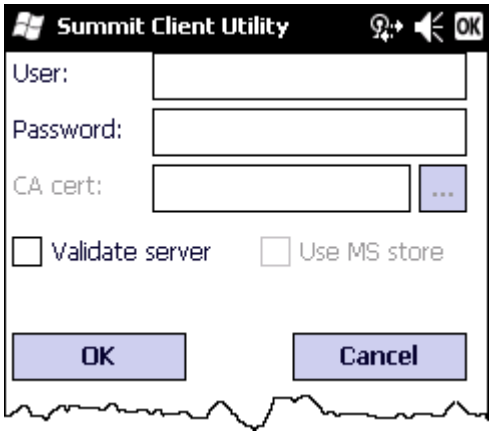
PEAP/MSCHAP

Note: The date must be properly set on the device to authenticate a certificate.

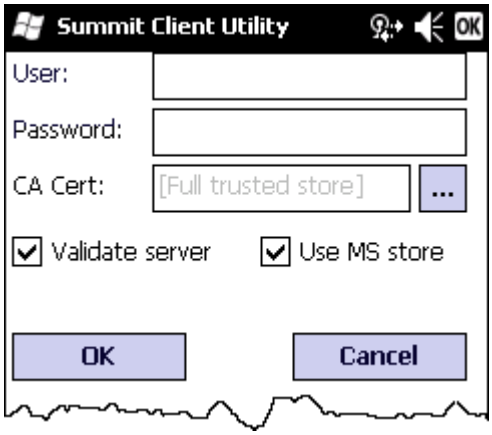
To use PEAP/MSCHAP, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile.
2. Set EAP Type to PEAP-MSCHAP.
3. Set Encryption to WPA TKIP.
4. Set Auth Type to Open.
5. To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.

6. See Sign-On vs. Stored Credentials (page 11-17) for information on entering credentials.
7. Tap the Credentials button.
   - No entries except the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name and Password when connecting to the network.
   - For Stored Credentials, User, Password and the CA Certificate Filename must be entered.
8. Enter these items as directed below.



9. Enter the Domain\Username (if the Domain is required), otherwise enter the Username.
10. Enter the password.
11. Leave the CA Certificate File Name blank for now.
12. Tap OK then tap Commit. Ensure the correct Active profile is selected on the Main Tab.
13. See Windows Certificate Store vs. Certs Path (page 11-19) for more information on certificate storage.
14. Once successfully authenticated, import the CA certificate into the Windows certificate store.
15. Return to the Credentials screen and check the Validate server check box.



If using the Windows certificate store:

1. Tap the Use MS store check box. The default is to use the Full Trusted Store.
2. To select an individual certificate, tap on the Browse button.
3. Uncheck the Use full trusted store check box.
4. Select the desired certificate and tap Select. You are returned to the Credentials screen.

If using the Certs Path option:

1. Leave the Use MS store box unchecked.
2. Enter the certificate filename in the CA Cert textbox.

After using the selected option (Windows certificate store or Certs Path), tap OK then tap Commit.

The device should be authenticating the server certificate and using PEAP/MSCHAP for the user authentication.

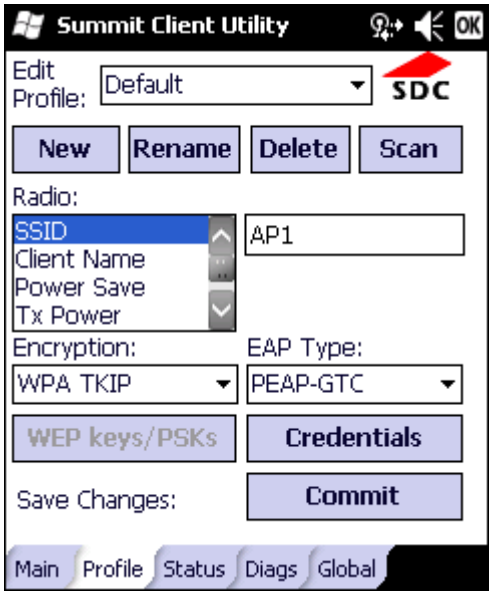
Ensure the correct Active Profile is selected on the Main Tab and perform a Suspend/Resume. The SCU Main tab shows the device is associated after the radio connects to the network.

PEAP/GTC

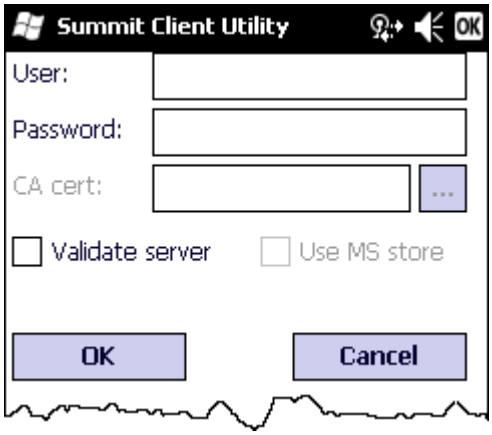
Note: The date must be properly set on the device to authenticate a certificate.

To use PEAP/GTC, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile.
2. Set EAP Type to PEAP-GTC.
3. Set Encryption to WPA TKIP.
4. Set Auth Type to Open.
5. To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.

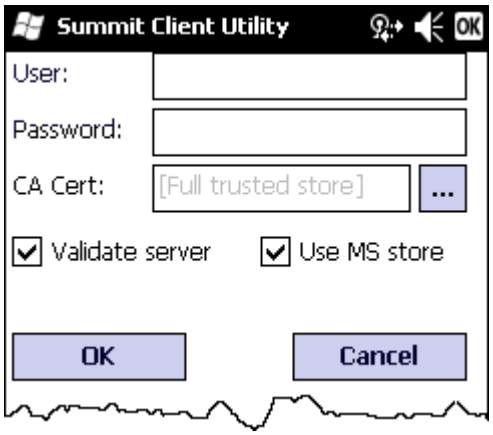


6. See Sign-On vs. Stored Credentials (page 11-17) for information on entering credentials.
7. Tap the Credentials button. No entries except the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name and Password when connecting to the network.
8. Enter these items as directed below.



9. Enter the Domain\Username (if the Domain is required), otherwise enter the Username.
10. Enter the password.

11. Leave the CA Certificate File Name blank for now.
12. Tap OK then tap Commit. Ensure the correct Active Profile is selected on the Main Tab.
13. See Windows Certificate Store vs. Certs Path (page 11-19) for more information on certificate storage.
14. Once successfully authenticated, import the CA certificate into the Windows certificate store.
15. Return to the Credentials screen and check the Validate server check box.



If using the Windows certificate store:

1. Tap the Use MS store check box. The default is to use the Full Trusted Store.
2. To select an individual certificate, tap on the Browse button.
3. Uncheck the Use full trusted store check box.
4. Select the desired certificate and tap Select. You are returned to the Credentials screen.

If using the Certs Path option:

1. Leave the Use MS store box unchecked.
2. Enter the certificate filename in the CA Cert textbox.

After using the selected option (Windows certificate store or Certs Path), tap OK then tap Commit.

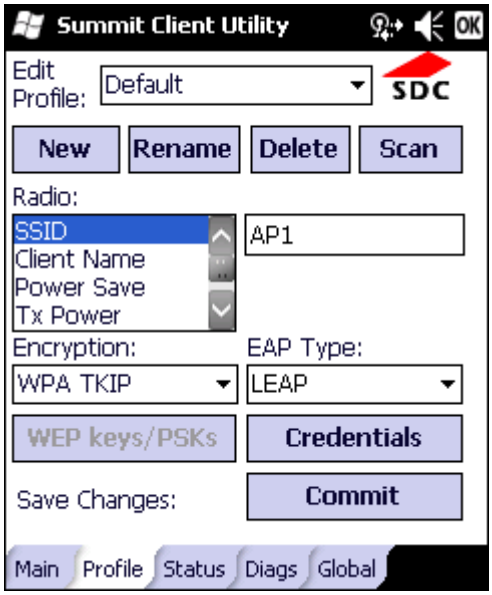
The device should be authenticating the server certificate and using PEAP/GTC for the user authentication.

Ensure the correct Active Profile is selected on the Main Tab and perform a Suspend/Resume. The SCU Main tab shows the device is associated after the radio connects to the network.

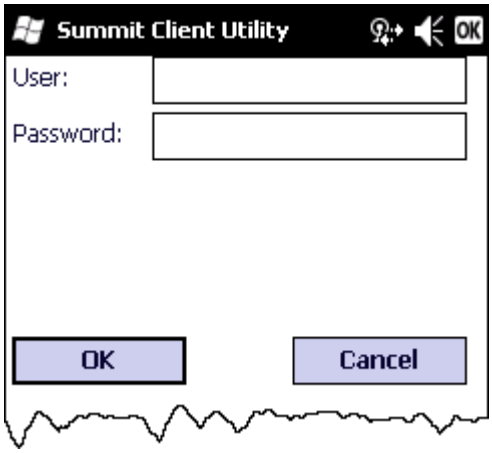
WPA/LEAP

To use WPA/LEAP, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile.
2. Set EAP Type to LEAP.
3. Set Encryption to WPA TKIP.
4. Set Auth Type as follows:
   - If the Cisco/CCX certified AP is configured for open authentication, set the Auth Type radio parameter to Open.
   - If the AP is configured to use shared key or passphrase, set the Auth Type radio parameter to Shared.
   - If the AP is configured for network EAP only, set the Auth Type radio parameter to LEAP.
5. To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.



6. See Sign-On vs. Stored Credentials (page 11-17) for information on entering credentials.
7. To use Stored Credentials, tap on the Credentials button. No entries are necessary for Sign-On Credentials as the user will be prompted for the Username and Password when connecting to the network.



8. Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

9. Enter the password.
10. Tap OK then tap the Commit button.
11. Ensure the correct Active Profile is selected on the Main Tab and perform a Suspend/Resume. The SCU Main tab shows the device is associated after the radio connects to the network.

EAP-FAST

The SCU supports EAP-FAST with automatic or manual PAC provisioning. With automatic PAC provisioning, the user credentials, whether entered on the saved credentials screen or the sign on screen, are sent to the RADIUS server. The RADIUS server must have auto provisioning enabled to send the PAC provisioning credentials to the MX7 Tecton.

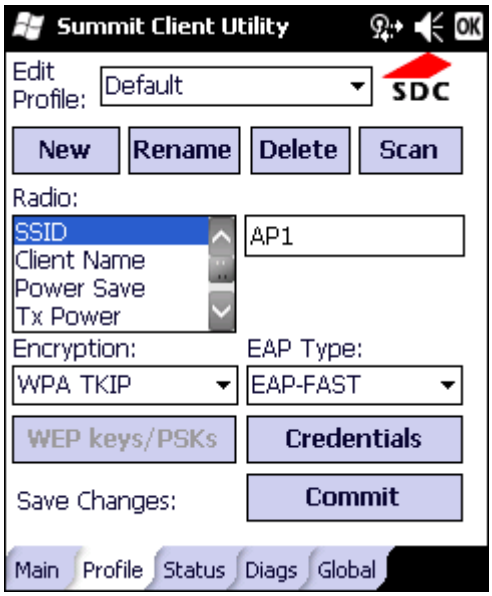
For automatic PAC provisioning, once a username/password is authenticated, the PAC information is stored on the MX7 Tecton. The same username/password must be used to authenticate each time. See the note below for more details.

Note: When using Automatic PAC Provisioning, once authenticated, there is a file stored in the \System folder with the PAC credentials. If the username is changed, that file must be deleted. The filename is autoP.00.pac.

For manual PAC provisioning, the PAC filename and Password must be entered.

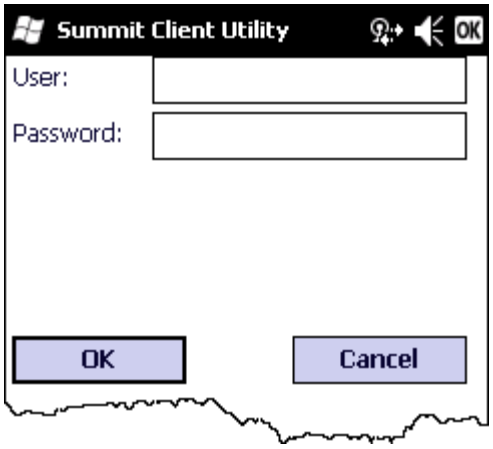
To use EAP-FAST, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile.
2. Set EAP Type to EAP-FAST.
3. Set Encryption to WPA TKIP.
4. Set Auth Type to Open.
5. To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.



6. See Sign-On vs. Stored Credentials (page 11-17)for information on entering credentials. The entries on the Credentials screen are determined by the type of credentials (stored or sign on) and the type of PAC provisioning (automatic or manual).
7. Tap on the Credentials button.

8. To use Stored Credentials, tap on the Credentials button. No entries are necessary for Sign-On Credentials with automatic PAC provisioning as the user will be prompted for the Username and Password when connecting to the network.



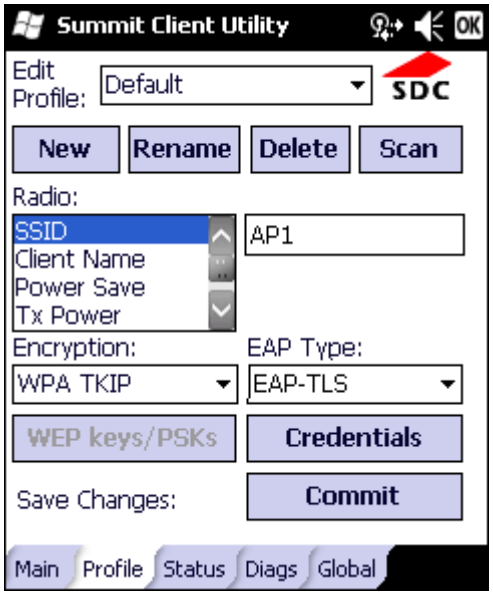
9. To use Sign-On credentials:
    - Do not enter a User and Password as the user will be prompted for the Username and Password when connecting to the network.
10. To use Stored Credentials:
    - Enter the Domain\Username (if the Domain is required), otherwise enter the Username.
    - Enter the password.
11. To use Automatic PAC Provisioning no additional entries are required.
12. To use manual PAC Provisioning:
    - Enter the PAC Filename and PAC Password.
    - The PAC file must be copied to the directory specified in the Certs Path global variable. The PAC file must not be read only.
13. Ensure the correct Active Profile is selected on the Main Tab and perform a Suspend/Resume. The SCU Main tab shows the device is associated after the radio connects to the network.

EAP-TLS

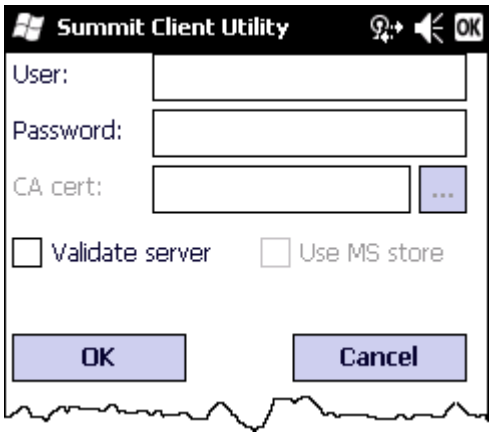
Note: The date must be properly set on the device to authenticate a certificate.

To use EAP-TLS, make sure the following profile options are used.

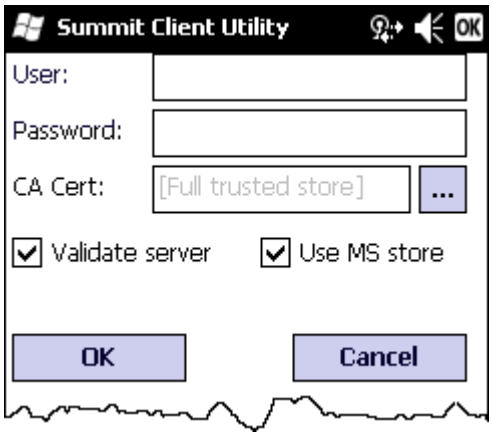
1. Enter the SSID of the Access Point assigned to this profile.
2. Set EAP Type to EAP-TLS.
3. Set Encryption to WPA TKIP.
4. Set Auth Type to Open.
5. To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.



6. See Sign-On vs. Stored Credentials (page 11-17) for information on entering credentials.
7. Tap the Credentials button.
   - No entries except the User Certificate Filename and the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name when connecting to the network.
   - For Stored Credentials, User and the CA Certificate Filename must be entered.
8. Enter these items as directed below.



9. Enter the Domain\Username (if the Domain is required), otherwise enter the User name.
10. Select a user certificate from the Windows certificate store. Use the Browse button to locate the User Cert from the certificate store. Highlight the desired certificate and press the Select button. The name of the certificate is displayed in the User Cert box.
11. Some versions of the SCU require a User Cert password. If this entry field is present, enter the password for the user certificate in the User Cert pwd box.
12. If there are no user certificates in the Windows certificate store, generate and install a user certificate.
13. See Windows Certificate Store vs. Certs Path (page 11-19) for more information on CA certificate storage.
14. Tap the Validate server check box.



If using the Windows certificate store:

1. Tap the Use MS store check box. The default is to use the Full Trusted Store.
2. To select an individual certificate, tap on the Browse button.
3. Uncheck the Use full trusted store check box.
4. Select the desired certificate and tap Select. You are returned to the Credentials screen.

If using the Certs Path option:

1. Leave the Use MS store box unchecked.
2. Enter the certificate filename in the CA Cert textbox.

After using the selected option (Windows certificate store or Certs Path), tap OK then tap Commit.

The MX7 Tecton should be authenticating the server certificate and using EAP-TLS for the user authentication.

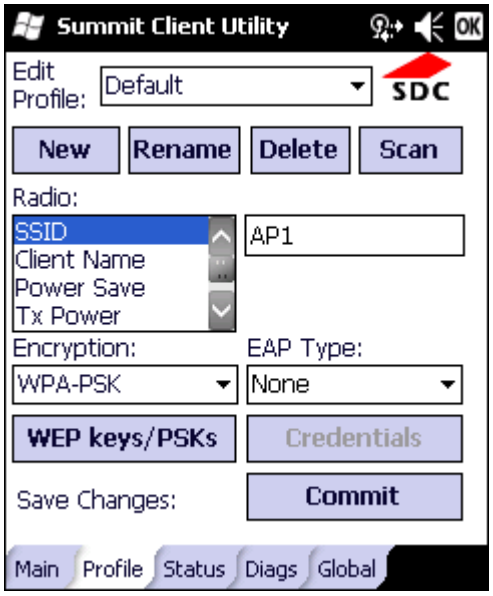
Ensure the correct Active Profile is selected on the Main Tab and perform a Suspend/Resume. The SCU Main tab shows the device is associated after the radio connects to the network.

Generate a Root CA certificate or a User certificate.

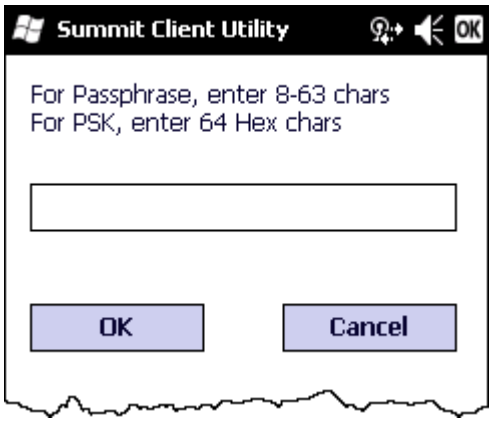
WPA PSK

To connect using WPA/PSK, make sure the following profile options are used:

1. Enter the SSID of the Access Point assigned to this profile.
2. Set EAP Type to None.
3. Set Encryption to WPA PSK or WPA2 PSK.
4. Set Auth Type to Open.



5. Tap the WEP keys/PSKs button.



6. This value can be 64 hex characters or an 8 to 63 byte ASCII value. Enter the key and tap OK.
7. Once configured, tap the Commit button.
8. Ensure the correct Active Profile is selected on the Main Tab and perform a Suspend/Resume. The SCU Main tab shows the device is associated after the radio connects to the network.

Certificates

Note: Refer to the Security Primer (available on the Honeywell web site) to prepare the Authentication Server and Access Point for communication.

Note: It is important that all dates are correct on the MX7 Tecton and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

Root Certificates are necessary for EAP-TLS, PEAP/GTC and PEAP/MSCHAP.

1. See Generating a Root CA Certificate (page 11-36) and download it to a PC.
2. Connect the MX7 Tecton to the desktop PC using ActiveSync and copy the certificate to the MX7 Tecton \System folder.
3. See Installing a Root CA Certificate (page 11-39) and install the Root CA Certificate.

User Certificates are necessary for EAP-TLS.

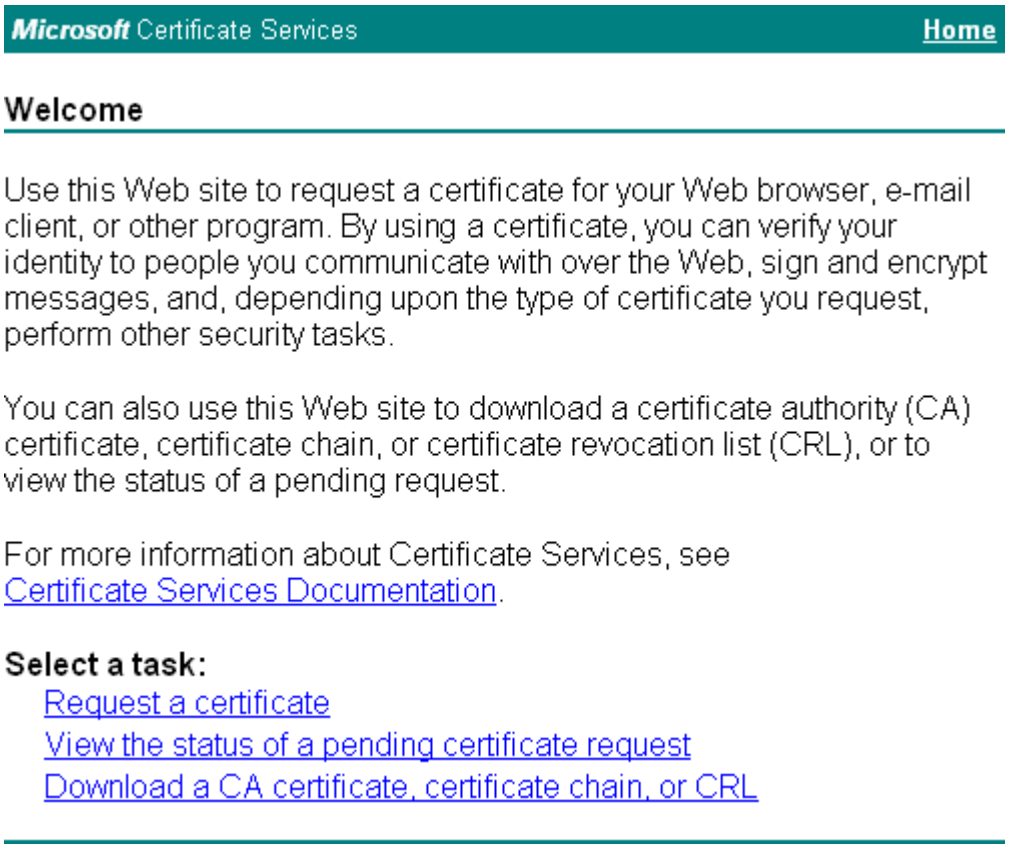
1. See Generating a User Certificate (page 11-39) and download it to a PC.
2. Install the User Certificate on the PC.
3. See Exporting a User Certificate (page 11-42) and export the User Certificate as a .PFX file.
4. Connect the MX7 Tecton to the desktop PC using ActiveSync and copy the certificate to the MX7 Tecton \System folder.
5. See Installing a User Certificate (page 11-43) and install the User Certificate.
6. After installation, perform a Suspend/Resume.
7. Verify Installation (page 11-43).

Generating a Root CA Certificate

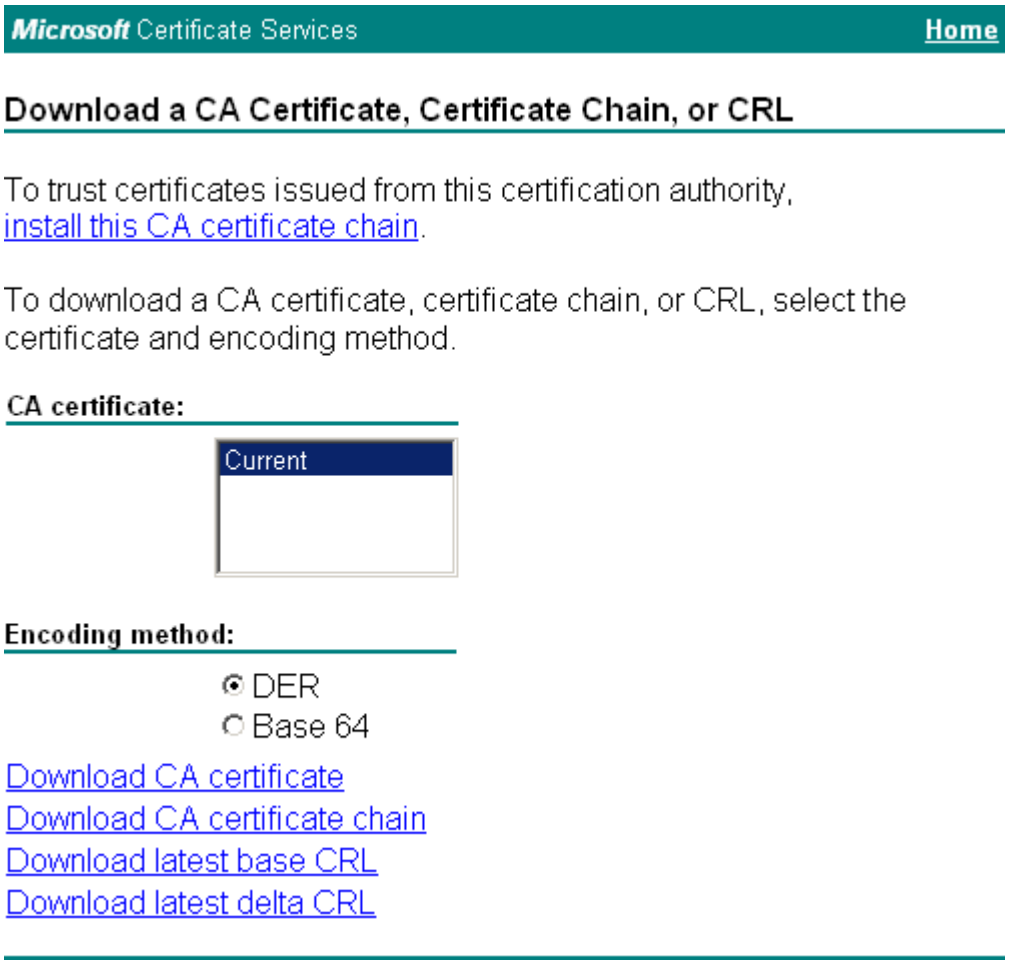
Note: It is important that all dates are correct on the MX7 Tecton and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

The easiest way to get the root CA certificate is to use a browser on a PC to navigate to the Certificate Authority.

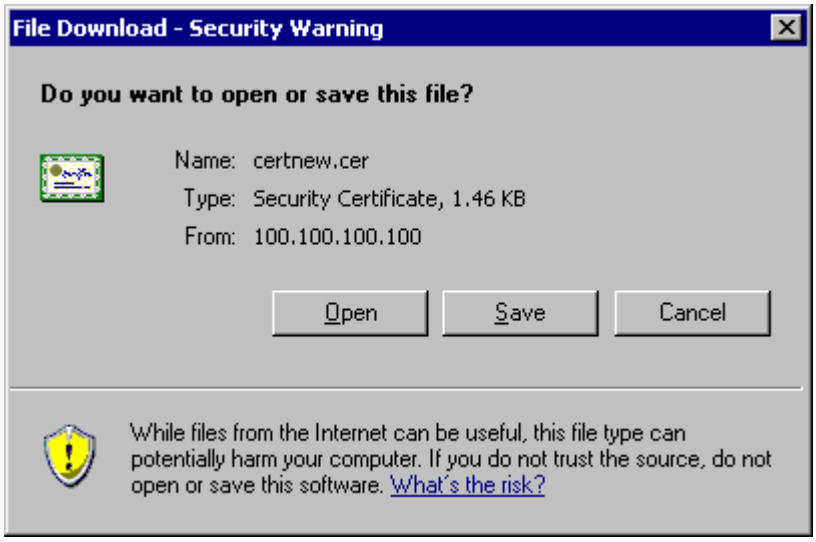
1. To request the root CA certificate, open a browser to http://<CA IP address>/certsrv.
2. Sign into the CA with any valid username and password.



3. Tap the Download a CA certificate, certificate chain or CRL link.
4. Make sure the correct root CA certificate is selected in the list box.



5. Tap the DER button.
6. To download the CA certificate, tap on the Download CA certificate link.



7. Tap the Save button and save the certificate. Make sure to keep track of the name and location of the certificate.

8. Install the Root CA Certificate on the MX7 Tecton.

Installing a Root CA Certificate

Note: This section is only if the Windows certificate store is used. If the certificate store is not used, copy the certificate to the \System folder or other path specified in the Summit Certs global parameter.

1. Copy the certificate file to the MX7 Tecton. The certificate file has a .CER extension. Locate the file and tap it.
2. A certificate installation warning text box is displayed:

   Your device is being asked to install a security certificate. You should block unless you require certificates for processes such as synchronizing with Exchange Server or connecting to a wireless network.
3. Tap More to view the remainder of the warning in the text box:

   Installing the certificate will cause your device to trust digital certificates from the requester. Malicious requesters may try to mislead you about their identity. Do you want to block this certificate?
4. Tap Install to continue the installation. An installation successful message is displayed.

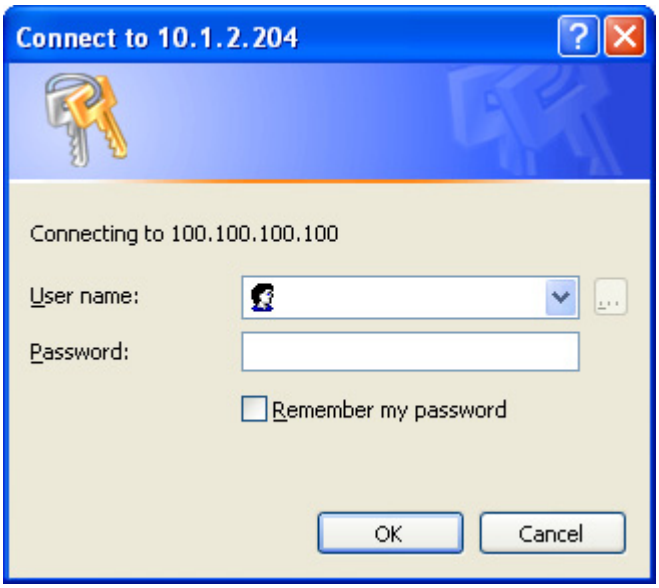
You can view any installed user certificates by selecting **Start > Settings > System** and tapping the Certificates icon.

Installed root certificates are displayed on the Root tab.

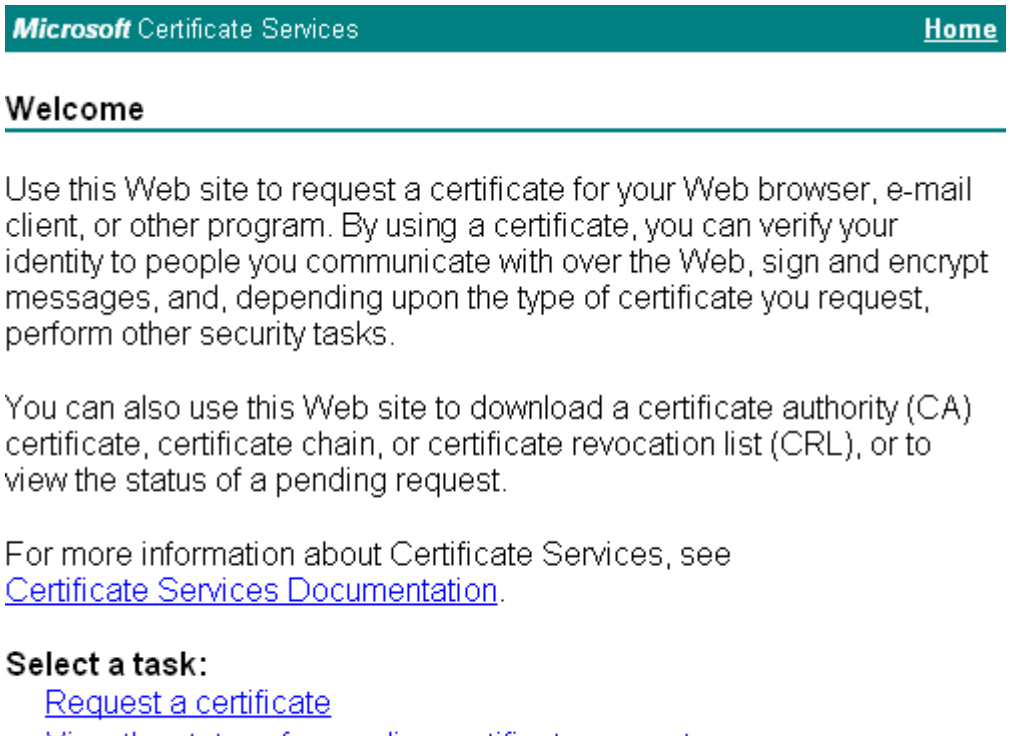
Generating a User Certificate

The easiest way to get the user certificate is to use the browser on a PC to navigate to the Certificate Authority.

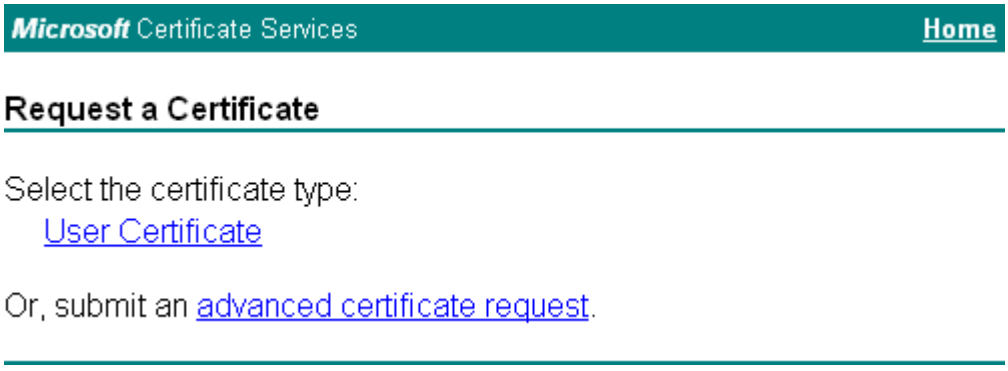
1. To request the user certificate, open a browser to http://<CA IP address>/certsrv.
2. Sign into the CA with the username and password of the person who will be logging into the mobile device.



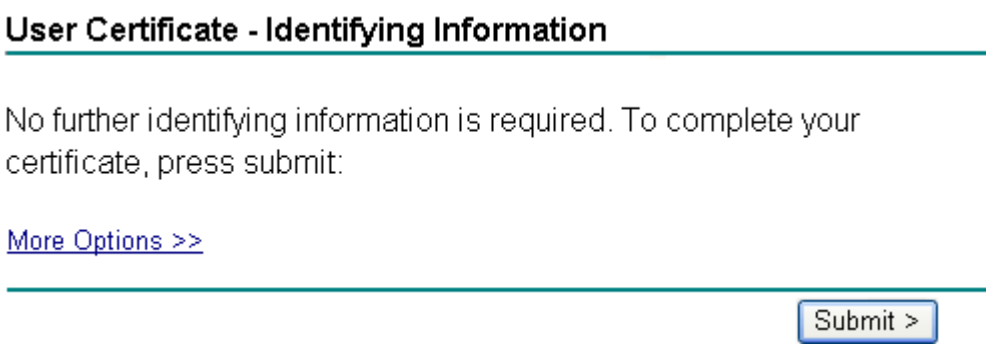
3. This process saves a user certificate file. A separate private key file is not required.



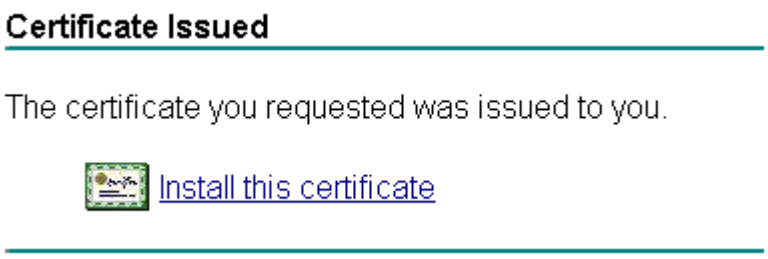
4. Tap the Request a certificate link.



5. Tap the User Certificate link.



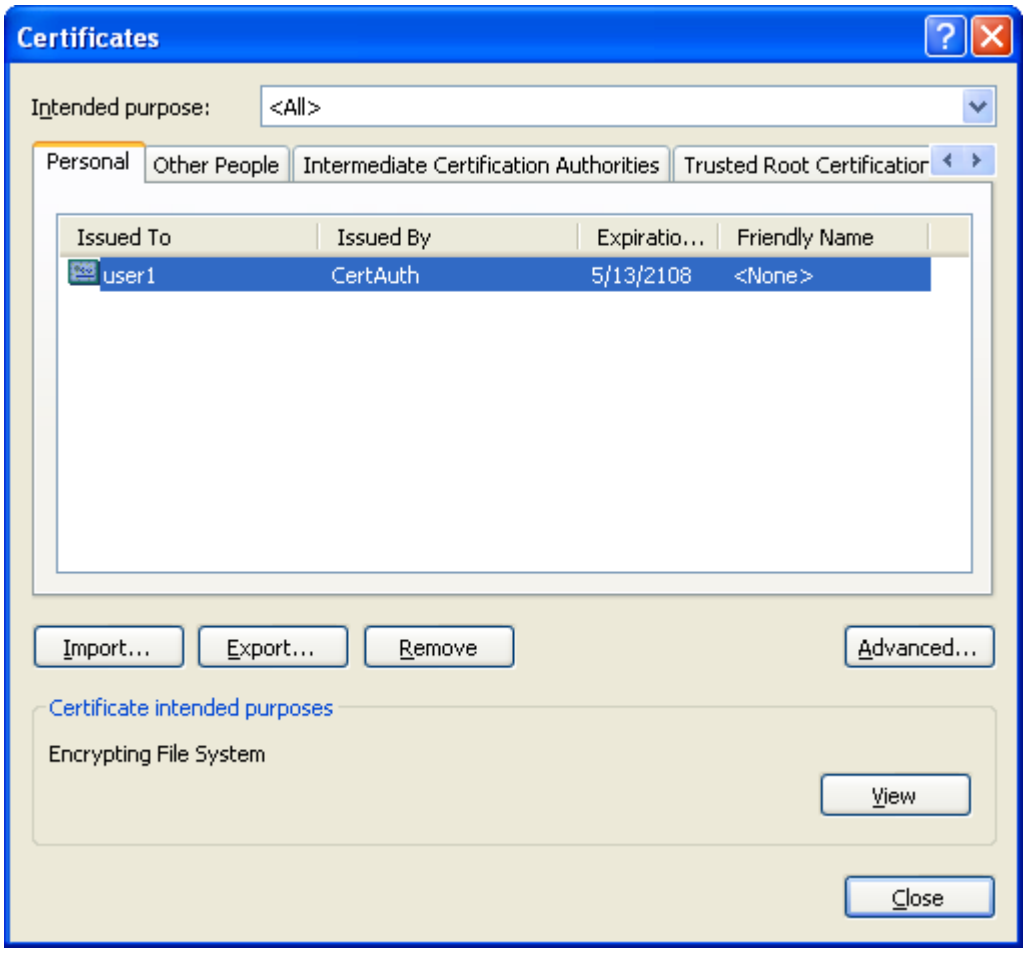
6. Tap on the Submit button. if there is a message box asking if you want to confirm the request, tap Yes.
7. The User Certificate is issued.



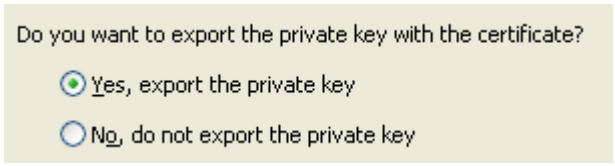
8. Install the user certificate on the requesting computer by tapping the Install this certificate link.
9. Export the certificate as described below.

Exporting a User Certificate

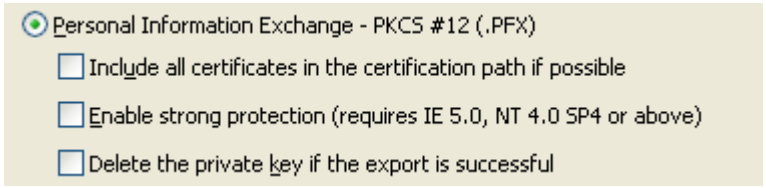
1. Start Internet Explore on the PC that requested the certificate.
2. Select **Tools > Internet Options > Content** and tap the **Certificates** button.



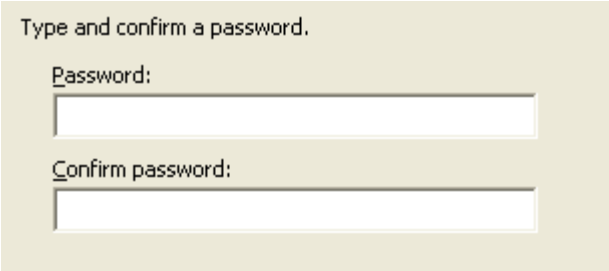
3. Make sure the Personal tab is selected. Highlight the certificate and tap the **Export** button.
4. The Certificate Export Wizard is started
5. Select **Yes**, export the private key and tap **Next**.



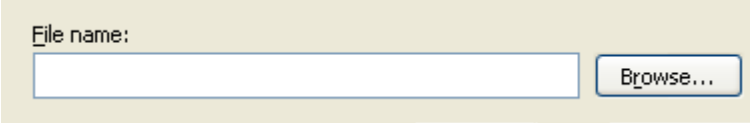
6. Uncheck **Enable strong protection** and check **Next**. The certificate type must be PKCS #12 (.PFX).



7. When the private key is exported, you must enter the password, confirm the password and tap Next. Be sure to remember the password as it is needed when installing the certificate.



8. Supply the file name for the certificate. Use the Browse button to select the folder where you wish to store the certificate. The certificate is saved with a .PFX extension.



9. Tap Finish and OK to close the Successful Export message.
10. Locate the User Certificate in the specified location. Copy to the MX7 Tecton.
11. Install the User Certificate.

Installing a User Certificate

1. After generating and exporting the user certificate, copy it from the PC to the MX7 Tecton. Copy the certificate to a location on the MX7 Tecton, such as a storage card or the \System folder.
2. Locate the certificate file (it has a .PFX extension) and tap on it. You are prompted for the password that was assigned when the certificate was exported.
3. Enter the password and tap Done. A message is displayed that the certificate installation was successful.

Verify Installation

1. You can view any installed user certificates by selecting **Start > Settings > System** and tapping the **Certificates** icon.
2. Installed user certificates are displayed on the Personal tab.

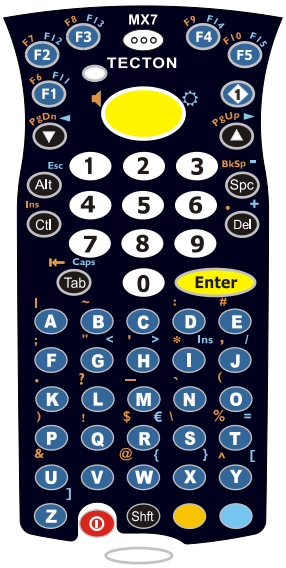
12 Keymaps

Introduction

Sticky keys are also known as *second function* keys. Ctl/Ctrl, Alt, Shft, Blue and Orange keys are sticky keys. Sticky keys do not need to be held down before pressing the next (or desired) key. You can use combined modifiers on specific keys.

The key mapping in this section relates to the physical Keypads (page 3-4). See the Input Panel for the Virtual (or Soft) Keypad used with the stylus.

55 key Alphanumeric Keymap - Primary Delete



- The following keymap is used on an MX7 Tecton that is NOT running a Terminal Emulator. Terminal emulators use a separate keymap.
- When using a sequence of keys that includes a sticky key, press the sticky key first, release it, then press the rest of the key sequence.
- When using a sequence of keys that includes the Orange or Blue keys, press the color key first then the rest of the key sequence.
- Tapping the Power key when in any sticky mode (Blue, Orange, Shift, etc.) either turns the device On (when Off) or places it in Suspend (when On).
- Alphabetic keys default to lower case letters. Press the Shft key, then the alphabetic key for an uppercase letter.
- The diamond 1, F1, F2, F3, F4 and F5 keys can be remapped using the Button panel (**Start > Settings > Personal > Buttons**).
- When the computer boots, the default condition of Caps (or CapsLock) is Off. The Caps (or CapsLock) condition can be toggled with Blue plus Tab key sequence.

To get this Key / Function	Press these Keys in this Order			
Power / Suspend	Power			
Field Exit (default VK_PAUSE) MAP = Mappable	Blue (MAP)	Orange (MAP)	Shift (MAP)	Diamond #1
Volume Adjust Mode	Orange	Scan	Up Arrow / Down Arrow	
Volume Adjust Mode	Blue	V	Up Arrow / Down Arrow	
Display Backlight Brightness Adjust Mode	Blue	Scan		
Toggle Blue Mode	Blue			
Toggle Orange Mode	Orange			
Toggle Shift Mode	Shft			
Alt	Alt			
Control	Ctl			
Esc	Blue	Alt		
Space	Spc			
Enter	Enter			
Scan	Scan			
CapsLock (Toggle)	Blue	Tab		
Back Space	Orange	Spc		

To get this Key / Function	Press these Keys in this Order			
Tab	Tab			
Back Tab	Orange	Tab		
Up Arrow	Up Arrow			
Down Arrow	Down Arrow			
Right Arrow	Right Arrow			
Left Arrow	Left Arrow			
Insert	Blue	I (letter i)		
Insert	Orange	Ctl		
Delete	Del			
Home	Shft	Down Arrow		
End	Shft	Up Arrow		
Page Up	Orange	Up Arrow		
Page Down	Orange	Down Arrow		
F1	F1			
F2	F2			
F3	F3			
F4	F4			
F5	F5			
F6	Orange	F1		
F7	Orange	F2		
F8	Orange	F3		
F9	Orange	F4		
F10	Orange	F5		
F11	Blue	F1		
F12	Blue	F2		
F13	Blue	F3		
F14	Blue	F4		
F15	Blue	F5		
F16	Shft	F1		
F17	Shft	F2		
F18	Shft	F3		
F19	Shft	F4		
F20	Shft	F5		
F21	Shft	Orange	F1	
F22	Shft	Orange	F2	
F23	Shft	Orange	F3	
F24	Shft	Orange	F4	
a	A			
b	B			
c	C			
d	D			

To get this Key / Function	Press these Keys in this Order			
e	E			
f	F			
g	G			
h	H			
i	I			
j	J			
k	K			
l	L			
m	M			
n	N			
o	O			
p	P			
q	Q			
r	R			
s	S			
t	T			
u	U			
v	V			
w	W			
x	X			
y	Y			
z	Z			
A	Shft	A		
B	Shft	B		
C	Shft	C		
D	Shft	D		
E	Shft	E		
F	Shft	F		
G	Shft	G		
H	Shft	H		
I	Shft	I		
J	Shft	J		
K	Shft	K		
L	Shft	L		
M	Shft	M		
N	Shft	N		
O	Shft	O		
P	Shft	P		
Q	Shft	Q		
R	Shft	R		
S	Shft	S		

To get this Key / Function	Press these Keys in this Order			
T	Shft	T		
U	Shft	U		
V	Shft	V		
W	Shft	W		
X	Shft	X		
Y	Shft	Y		
Z	Shft	Z		
1	1			
2	2			
3	3			
4	4			
5	5			
6	6			
7	7			
8	8			
9	9			
0	0			
. (period)	Orange	DEL		
. (period	Orange	K		
<	Blue	G		
[	Blue	Y		
]	Blue	Z		
>	Blue	H		
=	Blue	T		
{	Blue	W		
}	Blue	X		
/	Blue	J		
-	Blue	Spc		
+	Blue	Del		
* (asterisk)	Orange	I (letter i)		
* (asterisk)	Shft	8		
: (colon)	Orange	D		
; (semicolon)	Orange	F		
?	Orange	L		
` (accent)	Orange	N		
_ (underscore)	Orange	M		
, (comma)	Orange	J		
' (apostrophe)	Orange	H		
~ (tilde)	Orange	B		
\	Orange	S		
|	Orange	A		

To get this Key / Function	Press these Keys in this Order			
"	Orange	G		
!	Orange	Q		
!	Shft	1		
@	Orange	W		
@	Shft	2		
#	Orange	E		
#	Shft	3		
$	Orange	R		
$	Shft	4		
€	Blue	R		
%	Orange	T		
%	Shft	5		
^	Orange	Y		
^	Shft	6		
&	Orange	U		
&	Shft	7		
(	Orange	O		
(	Shft	9		
)	Orange	P		
)	Shft	0 (zero)		

55 Key 5250 Alphanumeric KeyMap - Primary Delete

- The following keymap is used on an MX7 Tecton that is running a 5250 Terminal Emulator.
- When using a sequence of keys that includes a sticky key, press the sticky key first, release it, then press the rest of the key sequence.
- When using a sequence of keys that includes the Orange or Blue keys, press the color key first then the rest of the key sequence.
- Tapping the Power key when in any sticky mode (Blue, Orange, Shift, etc.) either turns the device On (when Off) or places it in Suspend (when On).
- Alphabetic keys default to lower case letters. Press the Shft key, then the alphabetic key for an uppercase letter.
- The diamond 1, F1, F2, F3, F4 and F5 keys can be remapped using the Button panel (**Start > Settings > Personal > Buttons**).
- When the computer boots, the default condition of Caps (or CapsLock) is Off. The Caps (or CapsLock) condition can be toggled with Blue plus Tab key sequence

.

To get this 5250 Key / Function	**Press these Keys in this Order**			
Attn (Attention)	Ctl	A		
Clr (Clear)	Ctl	C		
Del (Delete)	Ctl	D		
Dup (Duplicate)	Ctl	U		
E-Inp (Erase Input)	Ctl	Q		
Field Exit (Enter)	Diamond 1			
Fld - (Field Minus)	Ctl	M		
Fld + (Field Plus)	Ctl	L		
Ins (Insert)	Ctl	I		
NL (New Line)	Ctl	N		
SysReq (System)	Ctl	S		
The following are ANSI keymaps				
Power / Suspend	Power			
Field Exit (default VK_PAUSE) MAP = Mappable	Blue (MAP)	Orange (MAP)	Shift (MAP)	Diamond #1
Volume Adjust Mode	Orange	Scan	Up Arrow / Down Arrow	
Volume Adjust Mode	Blue	V	Up Arrow / Down Arrow	
Display Backlight Brightness Adjust Mode	Blue	Scan		
Toggle Blue Mode	Blue			
Toggle Orange Mode	Orange			
Toggle Shift Mode	Shft			
Alt	Alt			
Control	Ctl			
Esc	Blue	Alt		

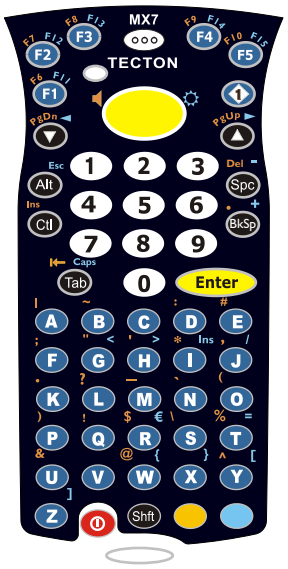
To get this 5250 Key / Function	Press these Keys in this Order			
Space	Spc			
Enter	Enter			
Scan	Scan			
CapsLock (Toggle)	Blue	Tab		
Back Space	Orange	Spc		
Tab	Tab			
Back Tab	Orange	Tab		
Up Arrow	Up Arrow			
Down Arrow	Down Arrow			
Right Arrow	Right Arrow			
Left Arrow	Left Arrow			
Insert	Blue	I (letter i)		
Insert	Orange	Ctl		
Delete	Del			
Home	Shft	Down Arrow		
End	Shft	Up Arrow		
Page Up	Orange	Up Arrow		
Page Down	Orange	Down Arrow		
F1	F1			
F2	F2			
F3	F3			
F4	F4			
F5	F5			
F6	Orange	F1		
F7	Orange	F2		
F8	Orange	F3		
F9	Orange	F4		
F10	Orange	F5		
F11	Blue	F1		
F12	Blue	F2		
F13	Blue	F3		
F14	Blue	F4		
F15	Blue	F5		
F16	Shft	F1		
F17	Shft	F2		
F18	Shft	F3		
F19	Shft	F4		
F20	Shft	F5		
F21	Shft	Orange	F1	
F22	Shft	Orange	F2	
F23	Shft	Orange	F3	

To get this 5250 Key / Function	Press these Keys in this Order			
F24	Shft	Orange	F4	
a	A			
b	B			
c	C			
d	D			
e	E			
f	F			
g	G			
h	H			
i	I			
j	J			
k	K			
l	L			
m	M			
n	N			
o	O			
p	P			
q	Q			
r	R			
s	S			
t	T			
u	U			
v	V			
w	W			
x	X			
y	Y			
z	Z			
A	Shft	A		
B	Shft	B		
C	Shft	C		
D	Shft	D		
E	Shft	E		
F	Shft	F		
G	Shft	G		
H	Shft	H		
I	Shft	I		
J	Shft	J		
K	Shft	K		
L	Shft	L		
M	Shft	M		
N	Shft	N		

To get this 5250 Key / Function	Press these Keys in this Order			
O	Shft	O		
P	Shft	P		
Q	Shft	Q		
R	Shft	R		
S	Shft	S		
T	Shft	T		
U	Shft	U		
V	Shft	V		
W	Shft	W		
X	Shft	X		
Y	Shft	Y		
Z	Shft	Z		
1	1			
2	2			
3	3			
4	4			
5	5			
6	6			
7	7			
8	8			
9	9			
0	0			
. (period)	Orange	DEL		
. (period	Orange	K		
<	Blue	G		
[	Blue	Y		
]	Blue	Z		
>	Blue	H		
=	Blue	T		
{	Blue	W		
}	Blue	X		
/	Blue	J		
-	Blue	Spc		
+	Blue	Del		
* (asterisk)	Orange	I (letter i)		
* (asterisk)	Shft	8		
: (colon)	Orange	D		
; (semicolon)	Orange	F		
?	Orange	L		
` (accent)	Orange	N		
_ (underscore)	Orange	M		

To get this 5250 Key / Function	Press these Keys in this Order			
, (comma)	Orange	J		
' (apostrophe)	Orange	H		
~ (tilde)	Orange	B		
\	Orange	S		
|	Orange	A		
"	Orange	G		
!	Orange	Q		
!	Shft	1		
@	Orange	W		
@	Shft	2		
#	Orange	E		
#	Shft	3		
$	Orange	R		
$	Shft	4		
€	Blue	R		
%	Orange	T		
%	Shft	5		
^	Orange	Y		
^	Shft	6		
&	Orange	U		
&	Shft	7		
(	Orange	O		
(	Shft	9		
)	Orange	P		
)	Shft	0 (zero)		

55 key Alphanumeric Keymap - Primary Backspace



Note: This keypad features a dedicated backspace key.

- The following keymap is used on an MX7 Tecton that is NOT running a Terminal Emulator. Terminal emulators use a separate keymap.
- When using a sequence of keys that includes a sticky key, press the sticky key first, release it, then press the rest of the key sequence.
- When using a sequence of keys that includes the Orange or Blue keys, press the color key first then the rest of the key sequence.
- Tapping the Power key when in any sticky mode (Blue, Orange, Shift, etc.) either turns the device On (when Off) or places it in Suspend (when On).
- Alphabetic keys default to lower case letters. Press the Shft key, then the alphabetic key for an uppercase letter.
- The diamond 1, F1, F2, F3, F4 and F5 keys can be remapped using the Button panel (**Start > Settings > Personal > Buttons**).
- When the computer boots, the default condition of Caps (or CapsLock) is Off. The Caps (or CapsLock) condition can be toggled with Blue plus Tab key sequence

.

To get this Key / Function	**Press these Keys in this Order**			
Power / Suspend	Power			
Field Exit (default VK_PAUSE) MAP = Mappable	Blue (MAP)	Orange (MAP)	Shift (MAP)	Diamond #1
Volume Adjust Mode	Orange	Scan	Up Arrow / Down Arrow	
Volume Adjust Mode	Blue	V	Up Arrow / Down Arrow	
Display Backlight Brightness Adjust Mode	Blue	Scan		
Toggle Blue Mode	Blue			
Toggle Orange Mode	Orange			
Toggle Shift Mode	Shft			
Alt	Alt			
Control	Ctl			
Esc	Blue	Alt		
Space	Spc			
Enter	Enter			
Scan	Scan			
CapsLock (Toggle)	Blue	Tab		
Back Space	Bksp			
Tab	Tab			
Back Tab	Orange	Tab		
Up Arrow	Up Arrow			
Down Arrow	Down Arrow			
Right Arrow	Right Arrow			
Left Arrow	Left Arrow			
Insert	Blue	I (letter i)		

To get this Key / Function	Press these Keys in this Order			
Insert	Orange	Ctl		
Delete	Orange	Spc		
Home	Shft	Down Arrow		
End	Shft	Up Arrow		
Page Up	Orange	Up Arrow		
Page Down	Orange	Down Arrow		
F1	F1			
F2	F2			
F3	F3			
F4	F4			
F5	F5			
F6	Orange	F1		
F7	Orange	F2		
F8	Orange	F3		
F9	Orange	F4		
F10	Orange	F5		
F11	Blue	F1		
F12	Blue	F2		
F13	Blue	F3		
F14	Blue	F4		
F15	Blue	F5		
F16	Shft	F1		
F17	Shft	F2		
F18	Shft	F3		
F19	Shft	F4		
F20	Shft	F5		
F21	Shft	Orange	F1	
F22	Shft	Orange	F2	
F23	Shft	Orange	F3	
F24	Shft	Orange	F4	
a	A			
b	B			
c	C			
d	D			
e	E			
f	F			
g	G			
h	H			
i	I			
j	J			
k	K			

To get this Key / Function	Press these Keys in this Order			
l	L			
m	M			
n	N			
o	O			
p	P			
q	Q			
r	R			
s	S			
t	T			
u	U			
v	V			
w	W			
x	X			
y	Y			
z	Z			
A	Shft	A		
B	Shft	B		
C	Shft	C		
D	Shft	D		
E	Shft	E		
F	Shft	F		
G	Shft	G		
H	Shft	H		
I	Shft	I		
J	Shft	J		
K	Shft	K		
L	Shft	L		
M	Shft	M		
N	Shft	N		
O	Shft	O		
P	Shft	P		
Q	Shft	Q		
R	Shft	R		
S	Shft	S		
T	Shft	T		
U	Shft	U		
V	Shft	V		
W	Shft	W		
X	Shft	X		
Y	Shft	Y		
Z	Shft	Z		

To get this Key / Function	Press these Keys in this Order			
1	1			
2	2			
3	3			
4	4			
5	5			
6	6			
7	7			
8	8			
9	9			
0	0			
. (period)	Orange	Bksp		
. (period	Orange	K		
<	Blue	G		
[	Blue	Y		
]	Blue	Z		
>	Blue	H		
=	Blue	T		
{	Blue	W		
}	Blue	X		
/	Blue	J		
-	Blue	Spc		
+	Blue	Bksp		
* (asterisk)	Orange	I (letter i)		
* (asterisk)	Shft	8		
: (colon)	Orange	D		
; (semicolon)	Orange	F		
?	Orange	L		
` (accent)	Orange	N		
_ (underscore)	Orange	M		
, (comma)	Orange	J		
' (apostrophe)	Orange	H		
~ (tilde)	Orange	B		
\	Orange	S		
|	Orange	A		
"	Orange	G		
!	Orange	Q		
!	Shft	1		
@	Orange	W		
@	Shft	2		
#	Orange	E		
#	Shft	3		

To get this Key / Function	Press these Keys in this Order			
$	Orange	R		
$	Shft	4		
€	Blue	R		
%	Orange	T		
%	Shft	5		
^	Orange	Y		
^	Shft	6		
&	Orange	U		
&	Shft	7		
(	Orange	O		
(	Shft	9		
)	Orange	P		
)	Shft	0 (zero)		

32 key Numeric-Alpha Keymap

- The following keymap is used on an MX7 Tecton that is NOT running a Terminal Emulator. Terminal emulators use a separate keymap.
- When using a sequence of keys that require an alpha key, first press the Alph key. Use the Shft sticky key or the Caps key sequence (Blue+Tab) for upper case alphabetic characters.
- Pressing the Alph key forces “Alpha” mode for the 2,3,4,5,6,7,8, and 9 keys. The 1 and 0 keys continue to place a 1 and 0 into the text field.
- To create a combination of numbers and letters before pressing Enter, remember to tap the Alph key to toggle between Alpha and Numeric mode.
- When using a sequence of keys that do not include the Alph key but does include a sticky key, press the sticky key first then the rest of the key sequence.
- The diamond 1, F1, F2, F3, F4 and F5 keys can be remapped using the Button panel (**Start > Settings > Personal > Buttons**).
- Pressing the Power key when in any sticky mode (Blue, Orange, Shift, etc) either turns the device On (when Off) or places it in Suspend (when On).

.

To get this Key / Function	**Press these Keys in this Order**		
Power / Suspend	Power		
Field Exit (default is VK_PAUSE) MAP = Mappable	Blue (MAP)	Shft (MAP)	Diamond #1
=	Orange	Shft (MAP)	Diamond#2 Default is Mappable
(	Blue	Shft (MAP)	Diamond#2 Default is Mappable
!	Orange	Shft (MAP)	Diamond#3 Default is Mappable
)	Blue	Shft (MAP)	Diamond#3 Default is Mappable
Volume Adjust Mode	Orange	Scan	Up Arrow Down Arrow
Display Backlight Brightness Adjust Mode	Blue	Scan	Up Arrow Down Arrow
Toggle Alpha Mode	Alph		
Toggle Blue Mode	Blue		
Toggle Orange Mode	Orange		
Toggle Shift Mode	Shft		
Alt Mode	Alt		
Control Mode	Ctrl		
Esc	Blue	Alt	
Space	Spc		
Enter	Enter		
Scan Mode	Scan		
CapsLock (Toggle)	Blue	Tab	

To get this Key / Function	Press these Keys in this Order		
Back Space	Orange	Spc	
Tab	Tab		
Back Tab	Orange	Tab	
Up Arrow	Up Arrow		
Down Arrow	Down Arrow		
Right Arrow	Blue	Up Arrow	
Left Arrow	Blue	Down Arrow	
Insert	Orange	Ctrl	
Delete	Del		
Home	Shft	Down Arrow	
End	Shft	Up Arrow	
Page Up	Orange	Up Arrow	
Page Down	Orange	Down Arrow	
F1	F1		
F2	F2		
F3	F3		
F4	F4		
F5	F5		
F6	Orange	F1	
F7	Orange	F2	
F8	Orange	F3	
F9	Orange	F4	
F10	Orange	F5	
F11	Blue	F1	
F12	Blue	F2	
F13	Blue	F3	
F14	Blue	F4	
F15	Blue	F5	
F16	Shft	F1	
F17	Shft	F2	
F18	Shft	F3	
F19	Shft	F4	
F20	Shft	F5	
F21	Shft	Orange	F1
F22	Shft	Orange	F2
F23	Shft	Orange	F3
F24	Shft	Orange	F4
a	Alpha	2	
b	Alpha	22	
c	Alpha	222	
d	Alpha	3	

To get this Key / Function	Press these Keys in this Order		
e	Alpha	33	
f	Alpha	333	
g	Alpha	4	
h	Alpha	44	
i	Alpha	444	
j	Alpha	5	
k	Alpha	55	
l	Alpha	555	
m	Alpha	6	
n	Alpha	66	
o	Alpha	666	
p	Alpha	7	
q	Alpha	77	
r	Alpha	777	
s	Alpha	7777	
t	Alpha	8	
u	Alpha	88	
v	Alpha	888	
w	Alpha	9	
x	Alpha	99	
y	Alpha	999	
z	Alpha	9999	
A	Shft	Alpha	2
B	Shft	Alpha	22
C	Shft	Alpha	222
D	Shft	Alpha	3
E	Shft	Alpha	33
F	Shft	Alpha	333
G	Shft	Alpha	4
H	Shft	Alpha	44
I	Shft	Alpha	444
J	Shft	Alpha	5
K	Shft	Alpha	55
L	Shft	Alpha	555
M	Shft	Alpha	6
N	Shft	Alpha	66
O	Shft	Alpha	666
P	Shft	Alpha	7
Q	Shft	Alpha	77
R	Shft	Alpha	777
S	Shft	Alpha	7777

To get this Key / Function	Press these Keys in this Order		
T	Shft	Alpha	8
U	Shft	Alpha	88
V	Shft	Alpha	888
W	Shft	Alpha	9
X	Shft	Alpha	99
Y	Shft	Alpha	999
Z	Shft	Alpha	9999
1	1		
2	2		
3	3		
4	4		
5	5		
6	6		
7	7		
8	8		
9	9		
0	0		
. (period)	Orange	DEL	
<	Blue	7	
[	Blue	2	
[	Orange	2	
]	Blue	3	
]	Orange	3	
>	Blue	8	
=	Orange	Diamond#2	
{	Blue	4	
}	Blue	5	
/	Blue	1	
-	Blue	Spc	
+	Blue	Del	
* (asterisk)	Orange	Diamond#1	
* (asterisk)	Shft	8	
: (colon)	Orange	0	
; (semicolon)	Blue	0	
?	Orange	8	
` (accent)	Blue	6	
_ (underscore)	Orange	7	
, (comma)	Orange	6	
' (apostrophe)	Orange	Alph	
~ (tilde)	Blue	9	
\	Orange	1	

To get this Key / Function	Press these Keys in this Order		
|	Orange	Alt	
"	Blue	Alph	
!	Orange	Diamond#3	
!	Shft	1	
@	Orange	5	
@	Shft	2	
#	Orange	4	
#	Shft	3	
$	Orange	9	
$	Shft	4	
%	Shft	5	
^	Blue	Ctrl	
^	Shft	6	
&	Shft	7	
(	Blue	Diamond#2	
(	Shft	9	
)	Blue	Diamond#3	
)	Shft	0 (zero)	

13 Battery Charger

Unpacking your Battery Charger

After you open the shipping carton containing the product, take the following steps:

- Check for damage during shipment. Report damage immediately to the carrier who delivered the carton.
- Make sure the items in the carton match your order.
- Save the shipping container for later storage or shipping.

Introduction

The MX7 Tecton Battery Charger is designed to simultaneously charge four rechargeable Lithium Ion (Li-Ion) battery packs. The time required for charging is dependent upon the battery pack temperature and conditions.

The battery charger should be located in an area where it:

- Is well ventilated.
- Is not in high traffic areas.
- Locates or orients the AC cord so that it will not be stepped on, tripped over or subjected to damage or stress.
- Has enough clearance to allow easy access to the power port on the back of the device.
- Is protected from rain, dust, direct sunlight or inclement weather.

This device is intended for indoor use only and requires an indoor AC power source. The charger is not approved for use in Hazardous Locations.

This device cannot charge/recharge coin cell batteries sealed inside the mobile device, if any.

This chapter is intended to familiarize the user with the safety and operating instructions necessary to use the MX7 Tecton Battery Charger (Model MX7390CHARGER, MX7391CHARGER) to charge rechargeable lithium-ion battery packs (MX7A380BATT, MX7A381BATT, MX7392BATT, MX7393BATT, MX7A396BATT) .

This information should be readily available to all users and maintenance personnel using this battery charger.

Store the charger and batteries when not in use in a cool, dry, protected place.

Cautions and Warnings

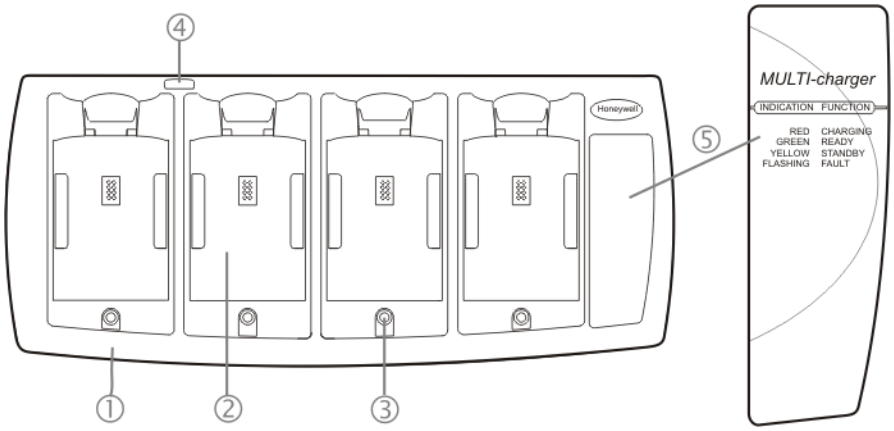
Battery Charger

- There is a risk of explosion if the MX7 Tecton Li-Ion battery in the charging pocket is replaced by an incorrect type. Other batteries or battery packs may burst causing injury or property damage.
- Do not insert any other type of Li-Ion battery in the battery charging pocket.
- Do not allow cleaning agents of any kind to contact the battery charging contacts; they may be damaged. If necessary, clean them with a soft-bristle, dry brush or compressed air.
- Disconnect the charger from AC power by pulling the plug; not the cord.
- Use care when inserting battery. Do not “slam” or slide the battery into the pocket, this could damage the charger.
- Keep dirt and foreign objects out of the battery pocket. Do not short circuit any of the contacts in the battery pocket, this could result in injury or property damage.
- Do not disassemble or perform modifications to the charger. There are no user serviceable components in the charger.

Lithium-Ion Battery Pack

- Dispose of used Li-Ion batteries according to the instructions for the type of battery.
- When not in use, lay the battery pack contact-side up in a protected environment.
- Do not store the Li-Ion battery pack in direct sunlight or anywhere the battery pack cannot cool down.
- If the Li-Ion battery pack is hot after removal from the MX7 Tecton, allow it to cool at room temperature or in a cool air stream before placing it in the charger.
- Do not dispose of Li-Ion batteries into a fire. Burning will generate hazardous vapors and may cause the battery to explode. Failure to observe this warning may result in injury from inhalation of vapors or burns from flying debris.
- Do not immerse Li-Ion batteries in water or any other liquid. If batteries are immersed, contact Technical Assistance (page 16-1).
- Do not disassemble or perform modifications to the battery. There are no user serviceable components in the battery.
- Do not place the Li-Ion battery into a pocket or toolbox with conductive objects (coins, keys, tools, etc.). A Li-Ion battery placed on damp ground or grass could be electrically shorted.
- Do not store Li-Ion batteries above 140°F (60°C) for extended periods.
- Failure to observe these warnings could result in injury or damage to the battery from rapid discharge of energy or battery overheating.
- Electrolyte Burns. Be careful when handling batteries. If a battery is broken or shows signs of leakage do not attempt to charge it. Dispose of it! Lead and Nickel-based cells contain a chemical solution that burns skin, eyes, etc. Leakage from cells is the only possible way for such exposure to occur. In this event, rinse the affected area thoroughly with water. If the solution contacts the eyes, get immediate medical attention.
- Electrical Burns. Batteries are capable of delivering high currents when accidentally shorted. Accidental shorting can occur when contact is made with jewelry, metal surfaces, conductive tools, etc., making the objects very hot. Never place a charged battery in a pocket or case with keys, coins, or other metal objects.

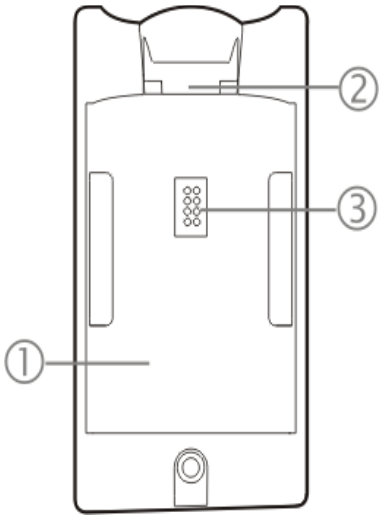
Front View



1. Front
2. Battery Charging Pocket
3. LED Indicator
4. Power Connection Location

LED Function Legend

Top View



1. Battery Charging Pocket
2. Retaining Clip
3. Battery Charging Contacts

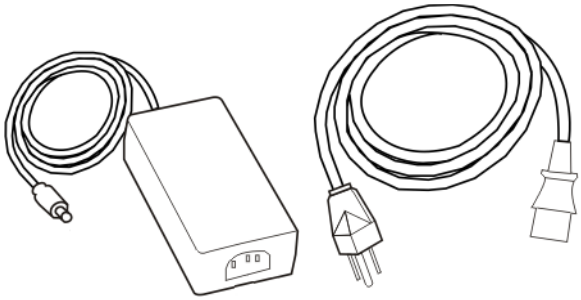
Installation

Assemble the Power Supply

Assemble the AC adapter for the MX7 Tecton Battery Charger before connecting it to the charger.

The AC power supply for the battery charger is shipped with the battery charger. Contact Technical Assistance (page 16-1) if there is no AC cable.

The battery charger power supply is intended for use with the MX7 Tecton battery charger *only.*



1. Plug the 3-prong end of the cable into an AC wall outlet.
2. Firmly press the female end of the power cable into the male connector on the AC power adapter. An LED on the power adapter illuminates when AC power is available.
3. AC power is now being applied to the power adapter.

Setup

Place the battery charger on a flat, horizontal, hard surface or fasten securely to a stable surface using the keyhole openings on the bottom of the battery charger. See Mounting (page 13-5).

Do not insert battery packs until the battery charger has finished powering up:

1. Assemble the Power Supply and connect it to an indoor power source (e.g. wall outlet).
2. Insert the power connector from the power supply into the power outlet at the back of the battery charger.
3. AC power is now being applied to the battery charger and it begins to power up.
4. Charge pocket LEDs flash while the battery charger enters and exits the startup check.
5. When the charge pocket LEDs are not illuminated, the battery charger is ready for use.

Mounting

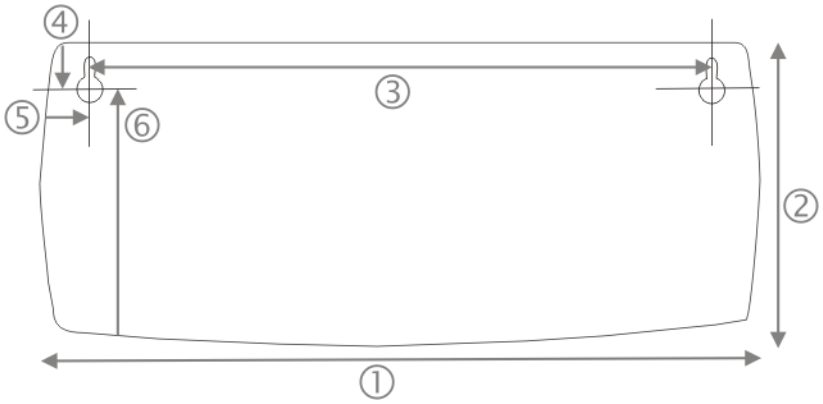
The battery charger should be located in an area where it:

- Is well ventilated.
- Is not in high traffic areas.
- Locates or orients the AC cord so that it will not be stepped on, tripped over or subjected to damage or stress.
- Has enough clearance to allow easy access to the power port on the back of the device.
- Is protected from rain, dust, direct sunlight or inclement weather.

This device is intended for indoor use only and requires an indoor AC power source. The charger is not approved for use in hazardous locations.

Place the battery charger on a flat, horizontal, hard surface.

The battery charger can be mounted to a stable, vertical surface (e.g., wall) using the keyhole openings in the bottom panel of the battery charger.

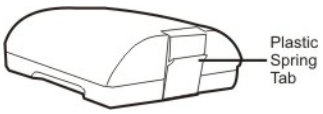


Note: Footprint is not to scale

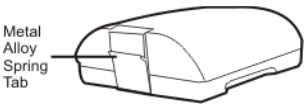
1. Length of battery charger - 11.75 inches (in)/ 29.8 centimeters (cm)
2. Width of battery charger - 5.25 in / 13.3 cm
3. Left keyhole center to right keyhole center - 9.8 in / 25 cm
4. Distance down to keyhole center from back of battery charger - 0.75 in / 1.9 cm
5. Distance to keyhole center from side of battery charger - 1.1 in / 3.0 cm
6. Distance to keyhole center from front of battery charger - 4.25 in / 10.8 cm

Care should be taken, when inserting batteries in a vertical-mounted battery charger, that the battery is secured by the latch in the battery charging pocket.

Charging Batteries



MX7A380BATT / MX7A381BATT



MX7392BATT / MX7393BATT / MX7396BATTERY

New batteries should be charged fully before first use. The life and capacity of a Lithium Ion battery pack can vary significantly depending on the discharge current and the environment in which it is used.

When a battery is placed in a charging pocket, the battery charger begins charging the battery. There is a slight delay while the charger evaluates the condition of the battery (ambient temperature, remaining charge, etc.) before charging begins.

As with all batteries, expect to see a reduction in the total number of operations a fully charged battery pack can deliver as it ages. When the battery reaches end of life (end-of-life occurs after 500 charge/discharge cycles) it must be replaced.

Battery packs do not need to be fully discharged between charge cycles.

While charging, the charger and battery pack will generate enough heat to feel warm. This is normal and does not indicate a problem.

Inserting a Battery into the Charging Pocket

It is important that battery packs are inserted into the charging pocket correctly. Inserting the battery incorrectly could result in damage to the battery pack or the charger.

Caution! Do not “slam” the battery pack into the charging pocket. Damage may result.

When preparing the battery pack for insertion into the battery charging pocket, hold the battery with its four charging contacts in line with the charging contacts in the charging pocket. Aim the retaining catch towards the back of the charger.

Tilt the front end (without the latch) of the battery pack into the front end of the battery charging pocket, and firmly press the other end (with the latch) until it is fully inserted into the battery charging pocket. Push down on the battery pack until the retaining clip on the battery catches on the retaining bracket in the pocket.

Remove the Battery from the Charging Pocket

Push the latch toward the battery and, grasping the battery and latch firmly, take the battery out of the charging pocket.

Interpreting the Charging Pocket LEDs

The status of the charge operation is indicated by the color of the LED for each charging pocket.

RED Continuous - on any charge pocket

Continuous red means the battery pack is charging.

RED FLASHING - on any charge pocket

Battery pack fault or failure.

RED FLASHING - on all charge pockets

Battery charger fault or failure.

Battery pack fault or failure or a battery charger timeout period expiration.

GREEN - on any charge pocket

Continuous green means the battery pack charge is complete - Battery is Ready.

YELLOW - on any charge pocket

Continuous yellow / amber means the battery pack temperature is out of range. The charging pocket is in standby mode while the pocket waits for the battery pack to warm up or cool down.

NO LIGHT - on any charge pocket

No light on a charge pocket means there is no battery pack installed,

- or the battery pack in the pocket is not fully inserted,
- or a defective or damaged battery pack is installed,
- or the charger is defective or damaged. Refer to Battery Charger Help.

NO LIGHT - on all charge pockets

No light means there is no AC power available to the battery charger or there is power but there are no batteries in any charging bay.

Battery Charger Help

The following is intended as an aid in determining whether the battery pack or the charger may be malfunctioning:

Problem	Cause	Solution
Battery pack does not fit in charging pocket.	Different manufacturer's battery pack, or there is an object in the charging pocket.	Check if the battery pack has part number MX-7A380BATT / MX7392BATT or a Low Temperature (CS) Battery : MX7A381BATT / MX7393BATT / MX7396BAT-TERY part number on the label. If not, do not use. Remove the object from the charging pocket.
No battery pack in charger, but any of the LEDs are on.	Dirt or foreign objects are in the charging pocket.	Unplug charger from AC supply. Remove any dirt or foreign objects from the charging pocket. See Charger Cleaning, Storage and Service (page 13-8). If the LEDs continue to remain ON, the charger may be defective. Return charger to an authorized service center.
Charger is plugged into a live outlet, battery pack is inserted, but RED LED is OFF and no other LEDs are on, or all LEDs are off.	Battery pack is not making contact with battery charge terminals in the charging pocket.	Push the battery pack in firmly until you hear a click as the battery catch connects with the charger pocket. Do not “slam” the battery pack into the charging pocket.
Charger is plugged into a live outlet, battery pack is inserted, but RED LED is OFF and no other LEDs are on, or all LEDs are off.	Faulty battery pack.	Replace battery pack.
Charger is plugged into a live outlet, battery pack is inserted, but RED LED is OFF and no other LEDs are on, or all LEDs are off.	New battery pack, same result.	Contact Technical Assistance (page 16-1) for replacement options.
When you first put a fully charged battery pack in the charging pocket, the RED LED comes on, indicating the battery pack is charging.	During the first few minutes, the battery charger checks the battery pack for correct voltage and charge state. During this time the LED is RED and is continuously ON. After charging is complete, the LED is GREEN.	There is nothing wrong with the battery pack or charger. Do not “top off” a fully charged battery pack by repeatedly placing it in the charging pocket. The battery pack may overheat and be damaged.
LED is flashing RED at any pocket.	Current could not be sourced through the battery pack due to age, exhaustion or damage to the cell(s). The battery pack does not communicate with the charger.	Contact Technical Assistance (page 16-1) for battery pack replacement options.
LED is flashing RED at any pocket.	The charger’s timeout period has expired.	Make sure that the battery pack temperature is within specification and retry charging. Contact Technical Assistance (page 16-1) if problem repeats, for battery pack replacement options.

Problem	Cause	Solution
LED is flashing RED at any pocket.	The battery pack voltage has not reached 6.0V within 30 minutes and the charger has timed out.	Contact Technical Assistance (page 16-1) for battery pack replacement options.
Solid YELLOW / AMBER LED when battery pack is inserted in the charging pocket.	The battery pack is too hot or too cold to charge.	Remove battery pack from the charging pocket and allow it to adjust to room temperature. *Note: If the battery pack is left in the charging pocket, it will cool down or warm to a temperature upon which the charger will begin the charge cycle. However, depending on the temperature of the battery, it may take 2-3 hours to adjust. The cool-down / warm-up of a battery pack is much quicker if the battery is not in the charging pocket.*

Charger Cleaning, Storage and Service

Cleaning

Unplug the charger from the power source before cleaning or removing debris from charging pockets.

Use only mild detergent with a slightly damp cloth to clean the outside of the charger. Do not use solvents or flammable cleaners. Allow the case to dry fully before using again.

Do not allow cleaning agents of any kind to contact the charging contacts; they may be damaged. If necessary, clean them with a soft-bristle, dry brush or compressed air.

Storage

Remove all batteries from the charging bays and disconnect AC power before placing the charger in storage. It should be stored in a cool, dry place, protected from weather and airborne debris.

Battery packs should be kept in a cool, dry place whenever possible. Do not store battery packs in direct sunlight, on a metal surface, or anywhere the battery pack cannot cool down. Do not leave the battery pack in a non-operating charger. The battery pack may discharge through the charger rather than hold its charge.

Service

There are no user serviceable parts in the rechargeable Lithium Ion battery or the charger. Contact Technical Assistance (page 16-1) should your charger require service.

Battery Cleaning, Storage and Service

Cleaning

The battery pack should not require cleaning unless it has become heavily soiled. Old or damaged batteries should be disposed of promptly and properly. The best way to dispose of used batteries is to recycle them. Battery recycling facilities recover the nickel, lithium or lead from old batteries to manufacture new batteries.

Use only mild detergent with a slightly damp cloth to clean the outside of the battery. Do not use solvents or flammable cleaners. Allow the case to dry fully before using again.

Do not allow cleaning agents of any kind to contact the charging contacts; they may be damaged. If necessary, clean them with a soft-bristle, dry brush or compressed air.

Storage

Battery packs should be stored, charging contact side up, in a cool dry place, protected from weather and airborne debris, whenever possible.

Do not store battery packs in direct sunlight, on a metal surface, or anywhere the battery pack cannot cool down.

Do not leave the battery pack in a non-operating charger. The battery pack may discharge through the charger rather than hold its charge.

Note: Battery packs may leak up to 1 mA current through the battery contacts when left in a non-powered charger pocket.

Service

There are no user serviceable parts in the lithium ion battery pack. Contact Technical Assistance (page 16-1) for battery disposal and replacement options.

14 Cradles

Unpacking your Cradles

After you open the shipping carton containing the product, take the following steps:

- Check for damage during shipment. Report damage immediately to the carrier who delivered the carton.
- Make sure the items in the carton match your order.
- Save the shipping container for later storage or shipping.

Communication cables and power cables are ordered separately.

Overview

This chapter provides instruction for the end-user, installer or system administrator to follow when setting up or using MX7 Tecton cradles.

Three cradles are available:

- A desktop cradle that secures the MX7 Tecton, recharges batteries and enables communications between the MX7 Tecton and another device. See Using a Desktop Cradle (page 14-3).
- A passive vehicle-mounted cradle that secures the MX7 Tecton and isolates it from shock and vibration. See Using a Passive Vehicle Cradle (page 14-14).
- A powered vehicle-mount cradle that secures the MX7 Tecton, isolates it from shock and vibration and recharges the battery. See Using a Powered Vehicle Cradle (page 14-18).

MX7 Tecton cradles are not certified for use in hazardous locations.

The MX7 Tecton must have a main battery installed when it is docked in a cradle. Wireless host/client communications can occur whether the cradle is receiving external power or not as wireless functions draw power from the main battery in the MX7 Tecton.

MX7 Tecton keypad data entries can be mixed with cradle-tethered scanner bar code data entries while the MX7 Tecton is in a powered cradle. Bluetooth device connection and use, while the MX7 Tecton is docked, are managed by the MX7 Tecton Bluetooth program, not the cradle.

The MX7 Tecton can be either On, Off or in Suspend Mode while in the cradle. Special purpose and power cables are available from Honeywell.

Never put the MX7 Tecton into a vehicle mounted assembly until the assembly is securely fastened to the vehicle.

Preparing the Cradle for Use

Note: Keep dirt and foreign objects out of the cradle. Do not short circuit any of the charging terminals (pins), as this action could result in injury or property damage.

Place cradles on a stable surface out of the way of:

- inclement weather,
- extremely high concentrations of dust or wind blown debris,
- accidental knocks, bumps or other shocks to the cradle and items in the cradle bays.
- Leave enough space at cable connectors to ensure cables are protected from jostling, tugging or being disconnected by passing objects.
- Leave enough space at the back of the cradle for the MX7 Tecton trigger handle.

In addition to the above, vehicle mounted cradles should be positioned in the vehicle where the cradle:

- is protected from rain and inclement weather,
- does not obstruct the driver's vision or safe vehicle operation,
- can be easily accessed by a user seated in the driver's seat while the vehicle is not in operation.

Tethered Scanners and the MX7 Tecton Cradles

An MX7 Tecton powered cradle supports tethered scanner attachment. A powered cradle provides 5V power to a tethered scanner. The passive vehicle cradle cannot support tethered scanner attachment. There is no software in the cradles.

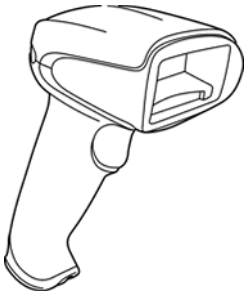
Note: The cradle must be powered by an external power source to enable tethered scanner use.

Note: Pressing the MX7 Tecton Scan button has no effect on tethered bar code scanners connected to a powered cradle. Tethered scanners read bar code scans only when the trigger on the tethered scanner is pressed.

A tethered scanner can be connected to the 9-pin RS232 Serial Interface port on the desktop cradle or to the Serial Interface port on the back of the vehicle cradle.

Bluetooth scanner connection and use, while the MX7 Tecton is docked in a cradle, are managed by the MX7 Tecton Bluetooth client, not the cradle.

MX7 Tecton keypad data entries can be mixed with tethered scanner bar code data entries. Any tethered scanner that decodes the bar code internally and outputs an RS232 data stream may be used. It sends the data to the MX7 Tecton in ASCII format.



Tethered scanners send scanned data to the MX7 Tecton when the MX7 Tecton is in a powered cradle and the tethered scanner is connected to the Serial Interface port on the cradle.

When a tethered scanner is connected to the Serial Interface port on a powered cradle, the MX7 Tecton must be configured as follows:

1. Open the Data Collection Wedge Main tab panel on the MX7 Tecton.
2. Enable either Device 1, Device 2 or Device 3.
3. Close the Data Collection Wedge application.

Maintenance

There are no serviceable parts in the MX7 Tecton cradles. Do not attempt to open the units.

If the cradle becomes cracked or broken at any time, it must be taken out of service and replaced. Contact Technical Assistance (page 16-1) for a replacement cradle.

Periodically test a mounted cradle and tighten connections as needed.

Cleaning

Do not use paper towels or harsh-chemical-based cleaning fluids since they may result in damage to the surfaces and/or battery connectors.

Use a clean soft cloth to wipe any dirt, moisture or grease from the MX7 Tecton, charging contacts or the cradle. Do not use any liquid to clean the cradle, battery pack, MX7 Tecton, or charging terminals (pins). Spray or dampen the cleaning cloth with liquids/sprays. If possible, clean only those areas which are soiled.

Lint/particulates can be removed from the connectors, charging terminals and charging/docking pockets with clean, filtered canned air.

Using a Desktop Cradle

Introduction

Note: When an external power supply is used to power this cradle, the external power supply should be UL Listed, with LPS or Class 2 outputs rated 12V, minimum 2 amps.

The desktop cradle is available in three configurations:

1. Without a power supply. A power supply must be ordered separately.
2. With a power supply and a US power cord.
3. With a power supply but without a power cord. A country specific power cord must be provided.

Communications cables for the MX7 Tecton are available separately.

Quick Start - Desktop Cradle

The following list outlines, in a general way, the process to follow when preparing the MX7 Tecton desktop cradle for use. Refer to the following sections in this document for more details.

1. Refer to Installing and Removing the Docking Bay Adapter Cup (page 14-7).
2. Connect the cradle end of the power adapter cable to the Power port on the back of the cradle.
3. Attach the AC power connector to a dependable power source.
4. Attach any desired external cabled devices to the ports on the cradle.
5. The desktop cradle is ready for use.

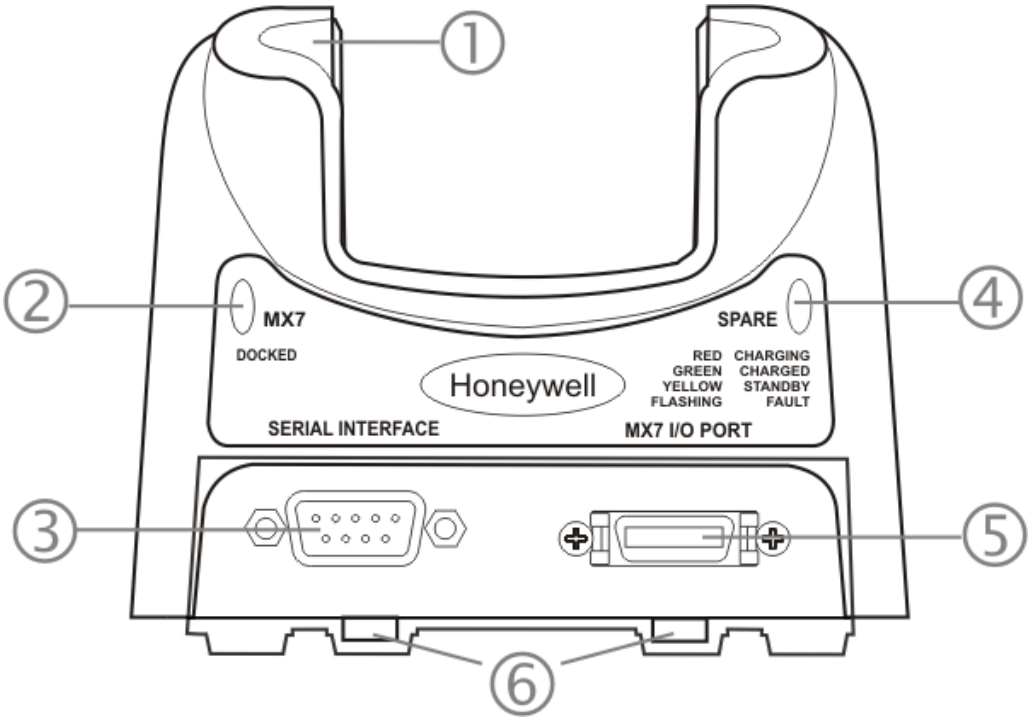
Battery Charging in a Desktop Cradle

The MX7 Tecton main battery recharging is managed by the Power Management settings in the MX7 Tecton. Refer to the Power control panel on the MX7 Tecton.

The spare battery in the spare battery well re-charges with or without an MX7 Tecton in the dock. The spare battery is fully charged in approximately four hours.

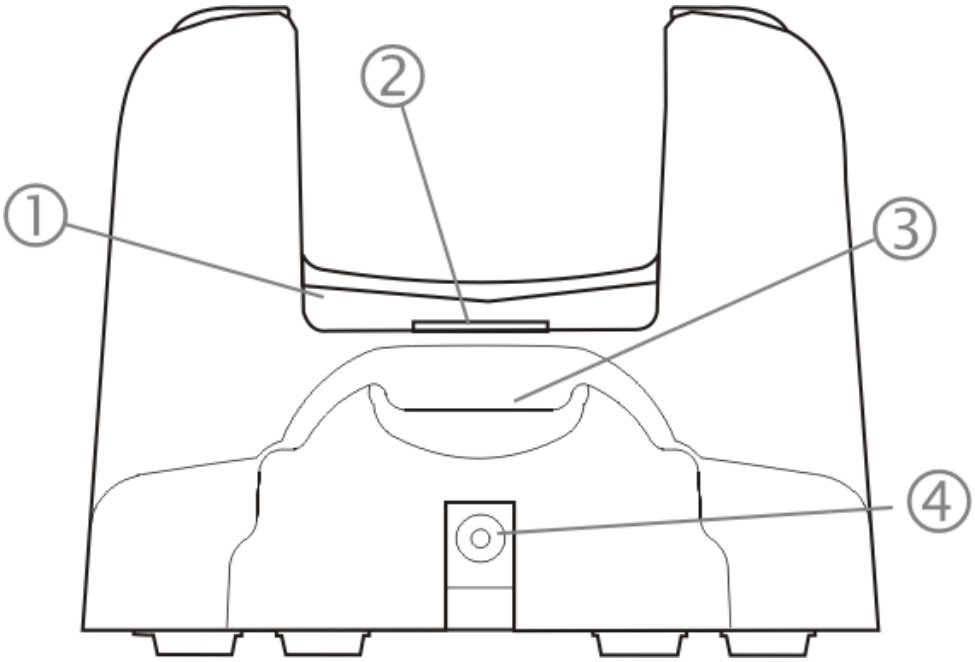
The cradle must be receiving power from an external power source before the main battery in the docked MX7 Tecton or spare battery pack charging can take place.

Front View



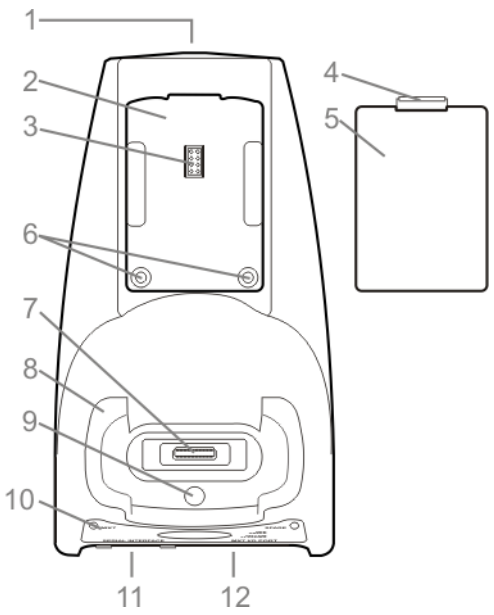
1. Charging Pocket Adapter Cup
2. MX7 Tecton Docked LED
3. Serial Interface Connector
4. Spare Battery LED
5. I/O Connector
6. Table Mounting Hole Guides

Back View



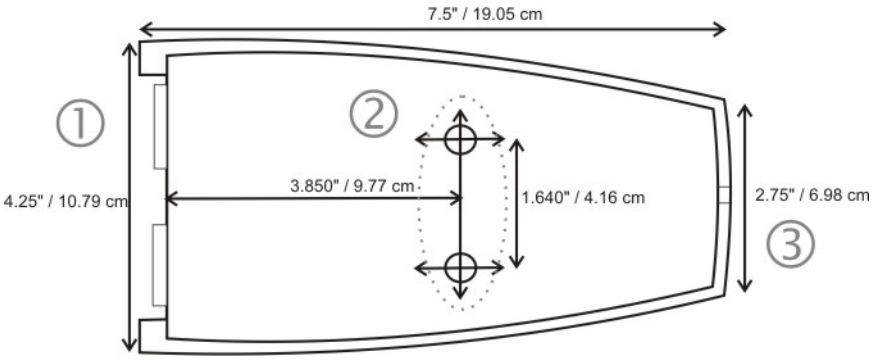
1. Charging Pocket Adapter Cup
2. Cradle Connector
3. Spare Battery Charging Bay
4. Power Connector

Top View



1. Power Supply Connector
2. Spare Battery Charging Bay
3. Spare Battery Charging Terminals
4. Spare Battery Latch
5. Spare Battery
6. Table Mounting Holes
7. Cradle Connector
8. Docking Bay Adapter Cup
9. Docking Bay Adapter Cup Mounting Hole
10. Desktop Cradle Label
11. Serial Interface Connector
12. I/O Connector

Desktop Mounting Footprint



1. Front
2. Table Mounting Hole Guides
3. Back

Bolts, washers, screws, screwdriver or wrench needed when attaching the MX7 Tecton desktop cradle to a protected flat surface are not supplied by Honeywell.

Periodically check the table mounting hardware and re-tighten if necessary. Table mounting hardware can be finger-tightened.

Note: Do not over-tighten the table mounting hardware. If the cradle is cracked, it must be replaced before being placed into service. Contact Technical Assistance (page 16-1) for help.

Installing and Removing the Docking Bay Adapter Cup

Equipment Required -- Phillips screwdriver and torquing tool (not supplied by Honeywell). You will need a torquing tool capable of torquing up to 6 (+/- .5) in/lb. Install/remove the docking bay adapter cup using a clean, well-lit stable surface.

The cradle is shipped with the docking bay adapter cup pre-installed. If the MX7 Tecton has a rubber boot, the docking bay adapter cup must be removed before the MX7 Tecton is placed in the desktop cradle.

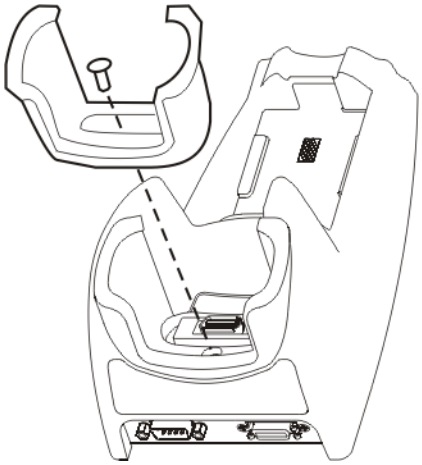
The cradles can dock an MX7 Tecton with a rubber boot (MX7490BOOT or MX7491BOOT) enclosing/protecting the device.

Before docking an MX7 Tecton without a rubber boot in the cradle, reinstall the docking bay adapter cup.

Installing

The adapter cup is installed facing in one direction.

1. Put the adapter cup in the MX7 Tecton docking bay, aligning the screw hole in the adapter cup with the screw hole in the MX7 Tecton docking bay.
2. Using a torquing screwdriver, insert the screw in the adapter cup screw hole, and torque the screw to 6 in/lbs +/- .5 in/lbs.
3. Periodically check the connection of the adapter cup and re-torque if necessary.



Removing

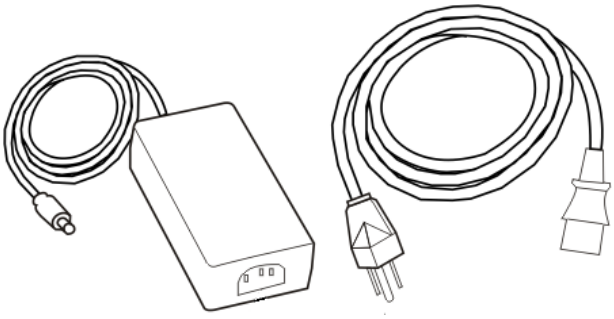
1. Remove the adapter cup by unscrewing the single captive screw at the front of the adapter cup.
2. Place both the adapter cup and the screw in a protected, safe area until needed.

Assemble/Attach the AC Power Adapter

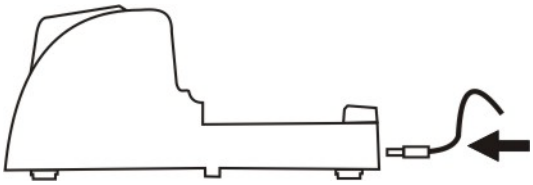
Note: Connect the cable to the cradle first, then to an AC source.

The external Power Supply for the cradle is shipped with the cradle. *Contact Technical Assistance* (page 16-1) if there is no AC cable.

The cradle Power connector is located on the back of the cradle.



1. Plug the AC power plug into any AC wall outlet with a dependable power source.
2. Firmly press the adapter end of the power cable into the 3 pin connector on the power adapter.
3. Firmly press the cradle end of the power cable into the single connector on the back of the cradle.
4. AC power is now being supplied to the AC power adapter and the cradle.

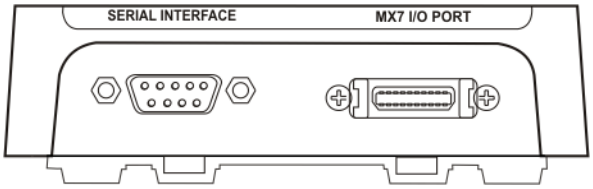


Connecting Input/Output Cables to the Desktop Cradle

Note: Route all cables to ensure they are protected from jostling, tugging or being disconnected by passing objects.

The cradle must be receiving power from an external power source before MX7 Tecton battery charging can begin.

The serial cable is connected to the port labeled Serial Interface on the left front of the desktop cradle. The serial cable end can originate with a tethered scanner, a PC, a printer or another serial device.



The I/O connector cable is connected to the port (male) labeled MX7 Tecton I/O Port on the right front of the desktop cradle.

Periodically test the connections for stability and re-tighten if necessary.

Attaching a Serial Cable

1. Align the RS232 serial cable end (female) carefully to the Serial Interface port (male) on the left front of the desktop cradle.
2. Press the ends together and finger tighten the screws on either side of the connector.
3. Test the connection for stability.

Attaching the Input/Output (I/O) Cable

1. Squeeze the clips next to the connector attached to the cable to open the catches in the connector assembly.
2. Firmly press the cable end (female) into the MX7 Tecton I/O Port connector (male) on the front of the cradle.
3. Release the clips in the connector cable.
4. Test the connection for stability.

Cradle LEDs

When the desktop cradle AC/DC power supply cable begins to supply power to the cradle, the cradle LEDs flash yellow, red, green for three seconds then turn off. The cradle is ready for use.

Docked LED

When Docked LED is …	It means ….
Off	MX7 Tecton not inserted or no power applied.
Red	MX7 Tecton docked and power applied.

Note: The cradle must be connected to a power source before the LEDs illuminate.

Spare Battery LED

When Spare LED is …	It means ….
Off	Battery pack not inserted or no power applied.
Green	Battery pack fully charged.
Red	Battery pack charging.
Yellow / Amber	Battery pack temperature out of range.
Flashing Red	Battery pack fault or failure.

Note: The cradle must be connected to AC power before the LEDs illuminate. Spare battery charging does not require an MX7 Tecton be docked in the docking bay.

MX7 Tecton System Status LED Status when Docked

The MX7 Tecton System Status LED is located above the Scan button.

When the MX7 Tecton LED is . . .	The Status is . . .	Comment
Blinking Red	Power Fail	Replace the main battery with a fully charged main battery. Or Connect the MX7 Tecton to external AC power to allow the internal charger to charge the main battery e.g., dock in a powered cradle.
Steady Red	Main Battery Low	Low Battery Warning. Replace the main battery with a fully charged main battery. Or dock the MX7 Tecton in a powered cradle.
Blinking Green	Display Off	No user intervention required.
No Color	Good	No user intervention required.

Docking and Undocking the MX7 Tecton

See Installing and Removing the Docking Bay Adapter Cup (page 14-7).

When the MX7 Tecton is in Suspend Mode it wakes up when it is docked in a powered cradle. There is no change in mode state settings or behavior when the MX7 Tecton is docked in a cradle without a power source.

MX7 Tecton mode states while the MX7 Tecton is in a powered cradle e.g., suspend, resume, display backlight, etc., are managed by the MX7 Tecton OS Power settings.

The MX7 Tecton is inserted into the charging pocket with the keypad facing forward. If the cradle is not permanently attached to the work surface, stabilize the cradle with one hand while inserting or removing the MX7 Tecton with the other hand.

Dock the MX7 Tecton

Remove any cables attached to the base of the MX7 Tecton.

Carefully press the MX7 Tecton straight down into the docking bay until the multi-pin connector at the base of the MX7 Tecton clicks into place with the multi-pin charging/communication connector at the bottom of the docking bay. The MX7 Tecton cradle is designed to secure the MX7 Tecton facing forward.

The cradle's Docked LED illuminates.

Undock the MX7 Tecton

Remove the MX7 Tecton from the cradle by pulling it straight up and out of the docking bay. If necessary, stabilize the cradle with one hand while the other hand removes the MX7 Tecton.

The cradle's Docked LED turns Off.

Inserting / Removing a Spare Battery from the Desktop Cradle

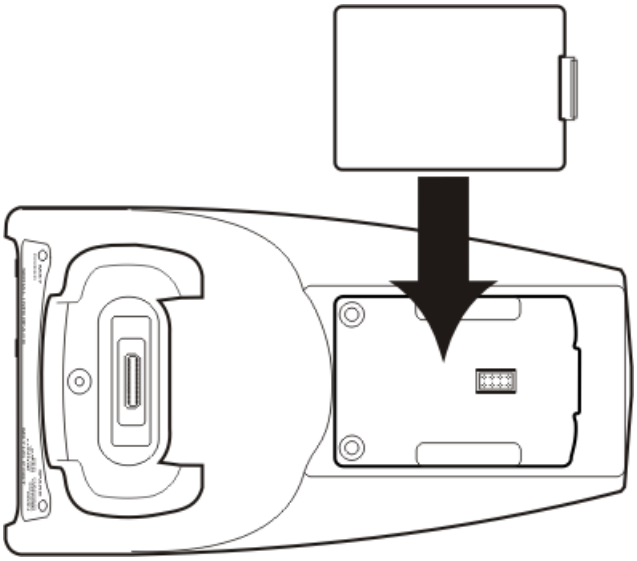
Prerequisites: The steps outlined in Assemble/Attach the AC Power Adapter (page 14-8) have been completed and the cradle has a dependable power source. The cradle has been bolted to a stable surface, if desired.

Note: Do not drop or slam the spare battery into the charging pocket. Damage may result.

A fully depleted spare battery recharges in approximately four hours in the MX7 Tecton powered cradle. Charging time may take longer if a tethered scanner, connected to the Serial port and drawing power from the cradle, is used.

The spare battery well is molded in the shape of the MX7 Tecton main battery. The spare battery can be inserted in the battery well in only one direction. When there is an MX7 Tecton, with or without a handle, docked in the cradle, a spare battery can still be inserted in the charging bay. You do not need to undock the MX7 Tecton before inserting or removing a spare battery in the cradle.

Stabilize the cradle with one hand when inserting/removing the spare battery, if necessary.



Inserting a Spare Battery

1. Hold the battery with the charging terminals facing down, toward the charging pocket.
2. Tilt the end (without the latch) of the spare battery pack into the upper end of the battery charging pocket, and firmly press down on the other end (with the latch) until the battery is fully inserted into the battery well.
3. Push down on the spare battery until the catch clicks into place, securing the spare battery in the battery bay. This will ensure the charging contacts on the spare battery connect with the re-charging contacts in the battery bay.

The Spare charging bay LED illuminates indicating the battery is properly seated in the charging bay.

Removing a Spare Battery

A green Spare battery LED signifies the spare battery is charged.

Remove the Spare battery by pushing the latch toward the battery and pulling the Spare battery up, with a hinging motion, and out of the charging bay. The Spare charging bay LED turns Off.

Desktop Cradle Help

The following is intended as an aid in determining whether the MX7 Tecton battery pack or the cradle battery charger may be malfunctioning.

Problem	Cause	Solution
Battery pack does not fit in battery well.	Different manufacturer's battery pack, or there is an object in the battery well.	Check if the battery pack is part number MX7A380BATT / MX7392BATT or a Low Temperature (CS) Battery : MX7A381BATT / MX7393BATT / MX7396BATTERY. If not, do not use. Remove the object from the battery well.
No battery pack in spare battery charging well, but the charging LED is on.	Dirt or foreign objects are in the battery well.	Unplug cradle from outlet. Remove any dirt or foreign objects from battery well. If the LED continues to stay ON, the cradle may be defective. Return charger to an authorized service center.
Cradle is plugged into a live outlet, battery pack is inserted, but RED LED is OFF and no other LEDs are on, or all LEDs are off.	Battery pack is not making contact with charging terminals in the battery well. Faulty battery pack. New battery pack, same result.	Push battery pack in firmly. Do not “slam” the battery pack into the battery well. Replace battery pack. Contact Technical Assistance (page 16-1) for replacement options.
When you first put a fully charged battery pack in the battery well, the RED LED comes on, indicating the battery pack is charging.	During the first few minutes, the charger checks the battery pack for correct voltage and charge state. During this time the LED is RED and is continuously ON. After charging is complete, the LED is GREEN.	There is nothing wrong with the battery pack or charging pocket.
LED is flashing RED at any station. LED is flashing RED at any station.	Current could not be sourced through the battery pack due to age, exhaustion or damage to the cell(s). Or The battery pack does not communicate with the charger.	Contact Technical Assistance (page 16-1) for battery pack replacement options.
	The charger’s timeout period has expired.	Make sure that the battery pack temperature is within specification and retry charging. If problem repeats, contact Technical Assistance (page 16-1) for battery pack replacement options.
Solid YELLOW LED when battery pack is inserted in the cradle.	The battery pack is too hot or too cold to charge.	Remove battery pack from the cradle and allow it to adjust to room temperature. If the battery pack is left in the cradle, it will cool down or warm to a temperature upon which the cradle will begin the charge cycle. However, depending on the temperature of the MX7 Tecton battery, it may take 2-3 hours to adjust. The battery pack can cool down faster if the battery is not in the battery well.
MX7 Tecton docked in cradle but cannot work with accessory cables connected to cradle.	MX7 Tecton not fully seated in cradle Foreign objects inside docking bay or cable connectors	Reseat the MX7 Tecton fully into the docking bay. Remove the foreign objects and reseat the MX7 Tecton into the docking bay.

Problem	Cause	Solution
MX7 Tecton docked in cradle but Docked LED does not light up.	MX7 Tecton not fully docked. Power supply not connected.	Check the docking bay is clear of foreign objects and reseat the MX7 Tecton fully into the docking bay. Check that power is applied to the Power Jack at the rear of the MX7 Tecton Desktop Cradle.

Using a Passive Vehicle Cradle

Introduction

Note: The protective boot or carrying case (if used) must be removed before inserting the MX7 Tecton into a securely mounted passive vehicle cradle.

The MX7 Tecton passive vehicle cradle consists of:

- Cradle bracket
- U-bracket
- 2 knobs
- Hook and loop fabric to secure the MX7 Tecton

An optional RAM assembly consists of:

- RAM ball base for vehicle mount
- RAM arm
- RAM base to attach U-bracket
- 4 each: bolts, nuts and washers

The installer must supply hardware to attach either the U-bracket or the RAM ball base to the vehicle.

Communications cables for the MX7 Tecton are available separately.

Wireless communication is available as long as the MX7 Tecton has sufficient energy in the main battery pack and a clear signal path. The passive vehicle cradle is lined with strips of hook-and-loop fabric to ensure a snug fit between the MX7 Tecton and the inside of the cradle. The cradle can secure the MX7 Tecton with or without a trigger or handstrap. The MX7 Tecton passive vehicle cradle does not have power, MX7 Tecton serial or input/output connectors.

There are two mounting options for the cradle:

- U-bracket mounting. See Installing the Cradle U-Bracket (page 14-16).
- RAM ball Arm mounting. See Installing the RAM Bracket (page 14-17).

Quick Start

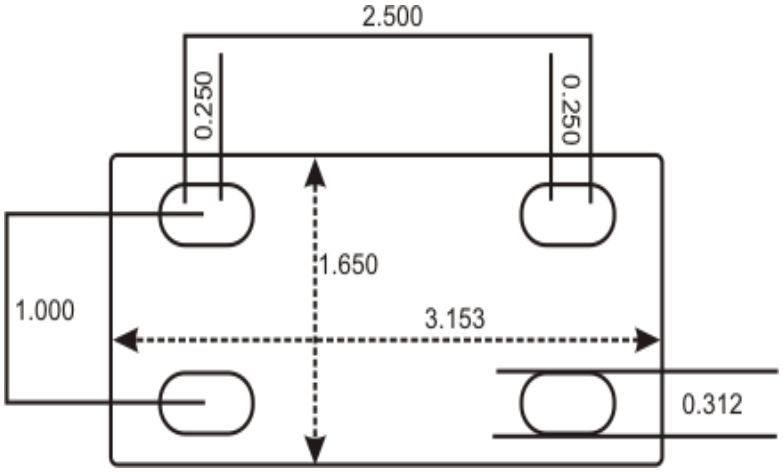
The following list outlines, in a general way, the process to follow when preparing the MX7 Tecton passive vehicle cradle for use. Refer to the following sections for more details.

1. Attach the RAM bracket or U-bracket mounting device to the vehicle.
2. Attach the MX7 Tecton passive cradle to the vehicle mounted bracket using the Angle Adjust knobs.
3. Adjust the cradle to the best viewing angle using the Angle Adjust knobs.

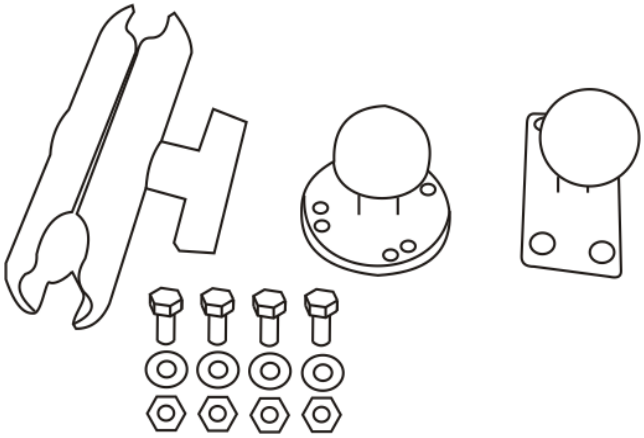
Components

U-Bracket Footprint

The image below is not to scale.



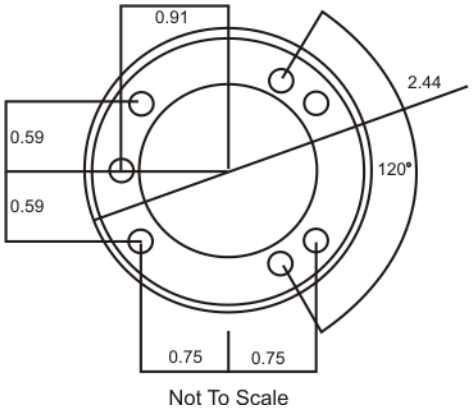
RAM Assembly Components

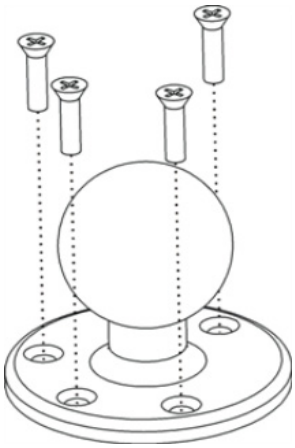


Mount the cradle U-bracket to the upper RAM ball assembly with the bolts, washers and nuts supplied by Honeywell.

- Qty 4 – Hex Cap 1/4-20 x 3/4 bolts
- Qty 4 – 1/4 flat washer
- Qty 4 – 1/4-20 nylon insert lock nuts

RAM Assembly Footprint

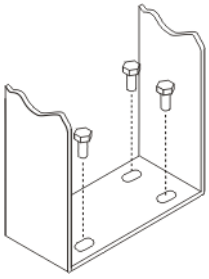




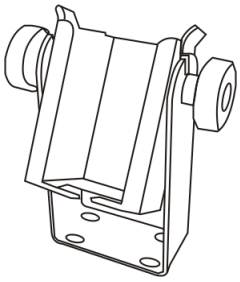
Installing the Cradle U-Bracket

Note: Honeywell does not supply the bolts or washers needed when mounting the cradle assembly to the vehicle chassis. Use bolts with a maximum 10/32" (0.3125) diameter.

1. Attach the U-Bracket to the vehicle, making sure it does not impede safe operation of the vehicle.



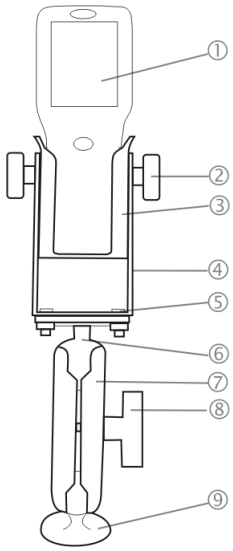
2. Attach the Passive Cradle to the U-Bracket using the Angle Adjust knobs.



3. Use both knobs to loosen and tighten the cradle to the U-bracket while determining the best viewing angle. The passive vehicle mounted cradle is ready for use.

Periodically test the passive mounting device and tighten bolts and/or knob as needed. If the cradle becomes cracked or warped it must be replaced before the cradle is put back in service.

Installing the RAM Bracket



1. MX7 Tecton
2. Angle Adjust Knobs
3. Passive Cradle
4. U-Bracket
5. Mounting Hex Bolt
6. Upper RAM Ball Assembly
7. Arm
8. Thumbscrew
9. Lower RAM Ball Assembly

1. Attach the lower RAM ball assembly to the vehicle, making sure it does not impede safe operation of the vehicle.
2. Fasten the upper RAM ball assembly to the base of the U-bracket using the supplied bolts, washers and screws.
3. Loosen the turnscrew on the RAM arm, place the lower socket over the vehicle mount RAM ball, then the other arm socket over the RAM ball on the U-bracket.

4. Tighten the arm turnscrew until the U-bracket is secured to the RAM arm and the vehicle.
5. Attach the Passive Cradle to the U-Bracket using the Angle Adjust knobs.
6. Use both knobs to loosen and tighten the cradle to the U-bracket while determining the best viewing angle. The passive vehicle mounted cradle is ready for use.

Periodically test the mounting device and tighten bolts and/or knob as needed. If the cradle becomes cracked or warped it must be replaced.

Using a Powered Vehicle Cradle

Introduction

The MX7 Tecton vehicle mount cradle uses one of the following power supply options:

- A power cable for 12V vehicles
- DC/DC power supply for non-12V vehicles
- AC/DC power supply with US power cord
- AC/DC power supply, requires country specific C14 type power cord.

The available RAM mount options include:

- RAM ball base for vehicle
- RAM ball base for MX7 Tecton
- 2 Screws (to attach RAM ball to MX7 Tecton)
- RAM arm

The installer must supply hardware to attach the RAM ball base to the vehicle.

Communications cables for the MX7 Tecton are available separately.

Quick Start

The following list outlines, in a general way, the process to follow when preparing the MX7 Tecton powered vehicle mounted cradle for use. Refer to the following sections for more details.

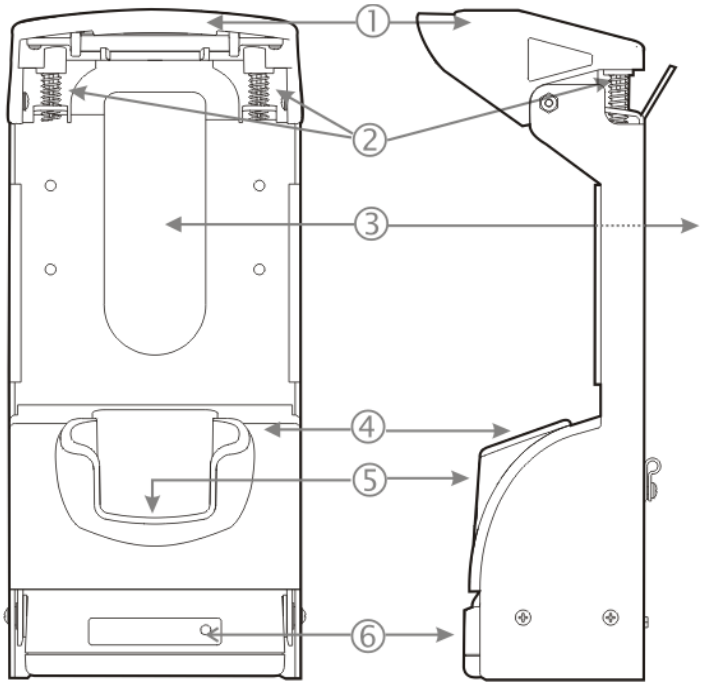
1. Attach the vehicle mounting assembly to the vehicle.
2. Attach the cradle to the vehicle mounting assembly.
3. Secure the MX7 Tecton in the mounted vehicle cradle.
4. Adjust the MX7 Tecton to the best viewing angle.
5. Connect peripheral cables.
6. Secure the DC/DC or 12 VDC power connector from the vehicle mounted power supply to the Power port.
7. Secure all cables in strain relief cable clamps.

The MX7 Tecton in the powered vehicle mounted assembly is ready for use.

Components

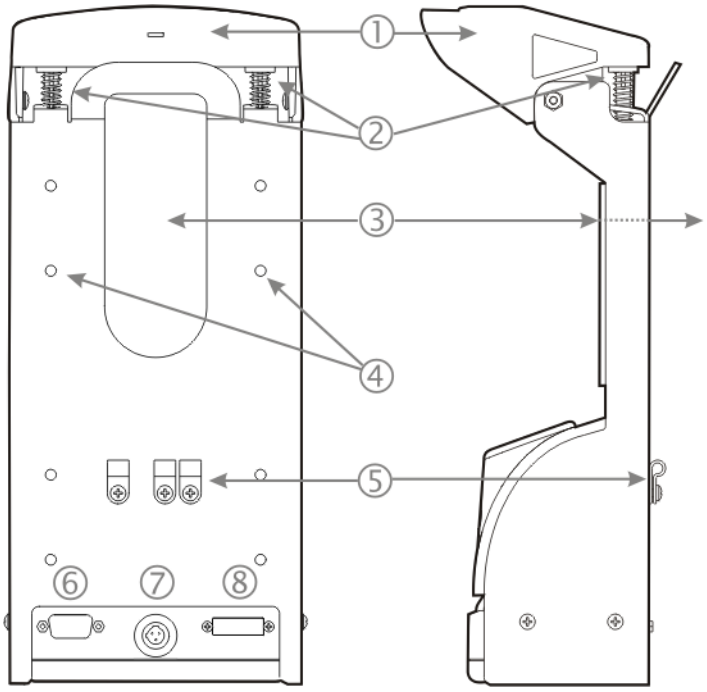
Before installation begins, verify you have the applicable vehicle mounting bracket assembly components necessary for your mount type.

Front View



1. Retainer
2. Retainer Springs
3. Handle Opening
4. Vehicle Cradle Adapter Cup
5. Charging Pocket
6. MX7 Tecton Docked LED

Back View

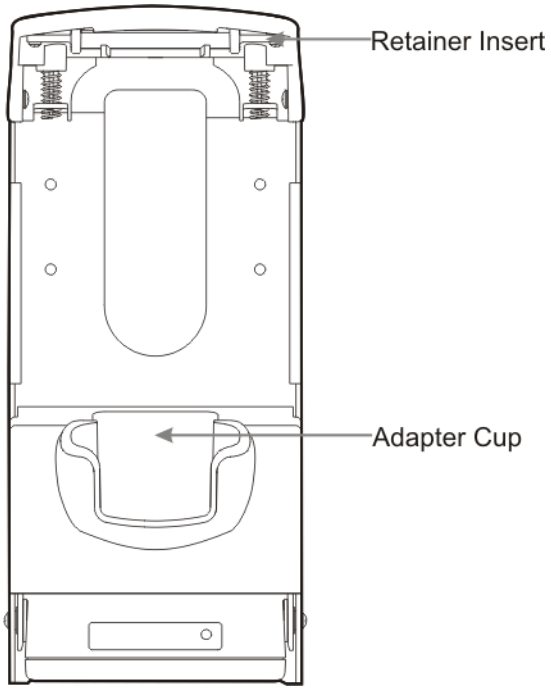


1. Retainer
2. Retainer Springs
3. Handle Opening
4. RAM Bracket Mounting Locations
5. Strain Relief Cable Clamps
6. Serial Interface Port
7. Power Connector
8. MX7 Tecton I/O Port

Installing or Removing Vehicle Cradle Adapter Cup and Top Adapter

Equipment Required -- Phillips screwdriver and torquing tool (not supplied by Honeywell). You will need a torquing tool capable of torquing up to 6 in/lb (+/- .5 in/lb) for the cradle adapter cup.

Install or remove the adapter on a clean, well-lit stable surface. The vehicle cradle is shipped with the cradle Adapter Cup and Retainer Insert pre-installed.

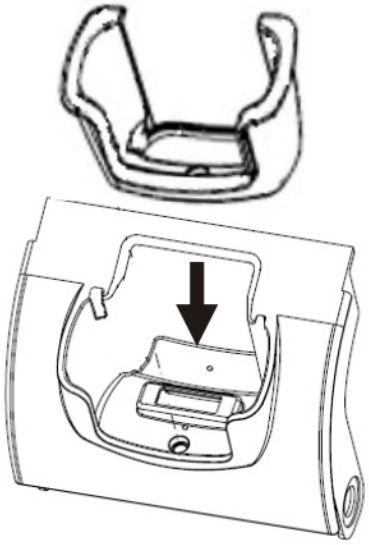


The MX7 Tecton cradle charging pocket, without a cradle adapter cup and top adapter, is designed for an MX7 Tecton with a rubber boot (MX7490BOOT or MX7491BOOT) enclosing/protecting the MX7 Tecton.

Before docking an MX7 Tecton without a rubber boot in the vehicle cradle, install the vehicle cradle Adapter Cup and Retainer Cap Insert.

Installing the Adapter

Charging Pocket Adapter Cup

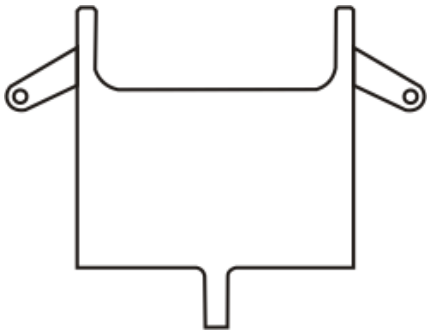


The adapter cup is installed facing in one direction.

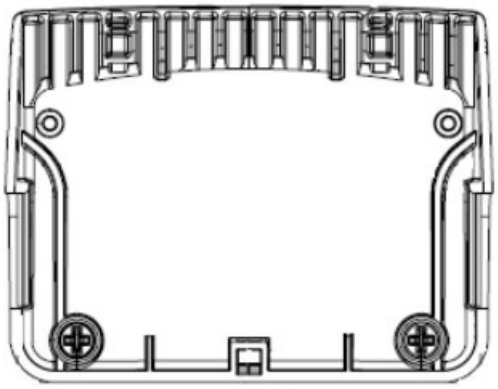
1. Slip the adapter cup into the cradle charging pocket, aligning the screw hole in the adapter cup with the screw hole in the charging bay.
2. Using a torquing screwdriver, insert the screw in the adapter cup screw hole, and torque the screw to 6 in/lbs +/- .5 in/lbs.

Retainer Insert

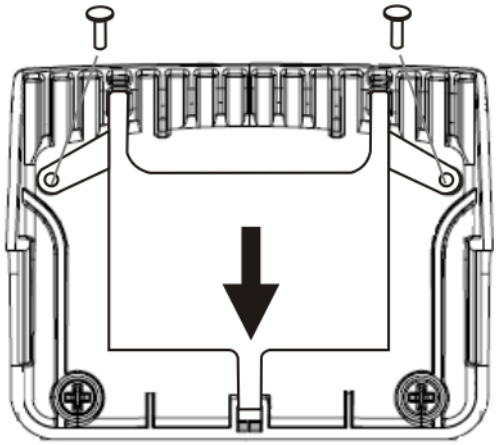
The Retainer Insert has three tabs.



1. Lay the flat side of the Retainer Insert against the underside of the Retainer cap, show below.



2. Slide the Retainer Insert back tab into the slot at the back of the Retainer.



3. Fasten the Retainer Insert to the Retainer cap using screws and the pre-drilled holes in the angled tabs (one on each side).
4. Fasten the Retainer Insert with two screws (the screws do not require a torquing tool).

Periodically check the connection of the adapter cup and re-torque if necessary. Periodically check the Retainer Insert connection and re-tighten if necessary.

Removing the Adapter Assembly

1. Remove the adapter cup by unscrewing the single captive screw at the front of the adapter cup.
2. Remove the Retainer Cap Insert by unscrewing the two screws holding it to the Retainer.
3. Slide the tab out of the slot in the back of the Retainer assembly.

Place the screws, adapter cups and the Retainer Cap Insert in a protected, safe place until needed.

If the adapter cup or retainer insert are cracked or broken, they must be replaced before a powered vehicle cradle, with an adapter cup and Retainer Cap Insert, is placed into service.

RAM Bracket Mounting

RAM Bracket Assembly mounting holes are on the back of the cradle. The mounting screws fit in Pim nuts and are automatically secured.

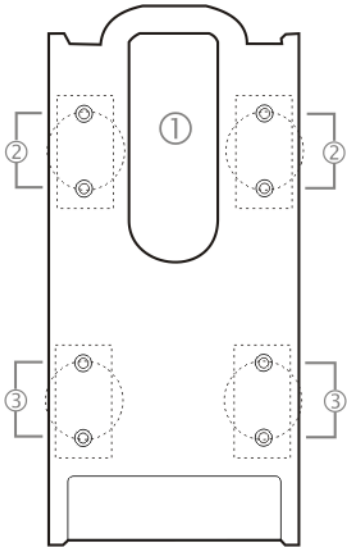
The number of RAM balls attached to the back of the vehicle mount cradle are dependent upon the desired RAM mount configuration.

The figure shown below is an example *only*.

RAM ball mounting screws are included in the mounting kit.

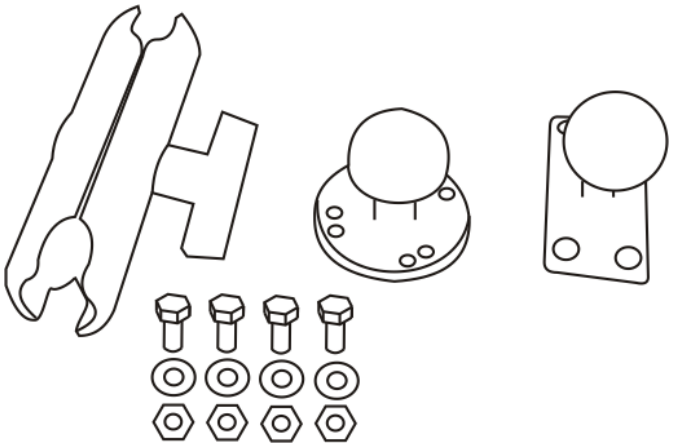
RAM Bracket Mounting Points

The figure shown below is an example *only*.



1. Trigger Handle opening
2. Upper mounting points
3. Lower mounting points

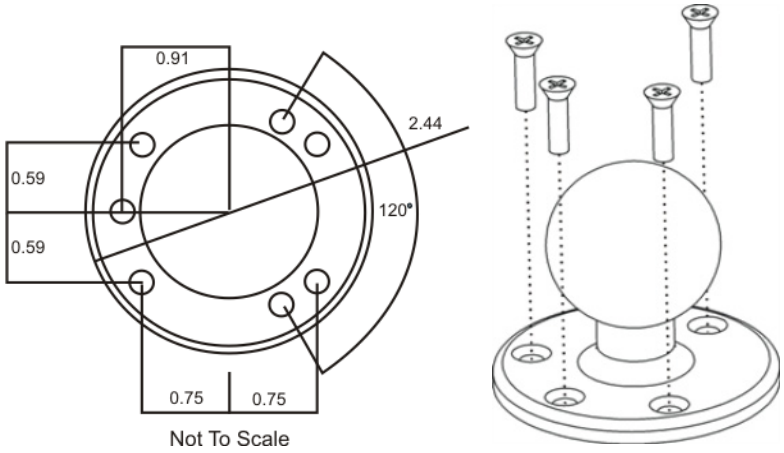
Vehicle Cradle RAM Ball Assembly



1. Fasten the RAM ball with the circular mounting base (shown in the middle in above image) to the vehicle.
2. Fasten the RAM ball with the rectangular mounting base (shown on the right in above image) to the back of the vehicle cradle.
3. Loosen the knob on the squeeze arm (shown on the left in above image).
4. Place either RAM ball opening in the squeeze arm over the vehicle mounted RAM ball.
5. Place the remaining RAM ball opening over the vehicle cradle mounted RAM ball.
6. Tighten the knob on the squeeze arm until the vehicle cradle is secured to the vehicle.
7. Adjust the position of the secured vehicle cradle by slightly loosening the squeeze arm knob, rotating the cradle and then re-tightening the squeeze arm knob.

Periodically test the mounting device and re-tighten bolts, RAM balls and/or squeeze arm adjustment knob as needed.

RAM Circular Base Footprint



Bolts, washers and nuts for mounting the RAM ball to the vehicle are supplied by Honeywell:

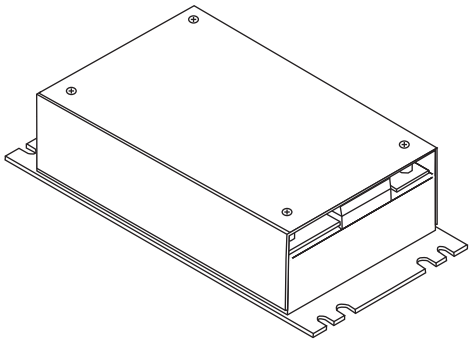
- Qty 4 – Hex Cap 1/4-20 x 3/4 bolts
- Qty 4 – 1/4 flat washer
- Qty 4 – 1/4-20 nylon insert lock nuts

Note: Mount to the most rigid surface available.

DC/DC Power Supply Installation, Screws on Top of lid

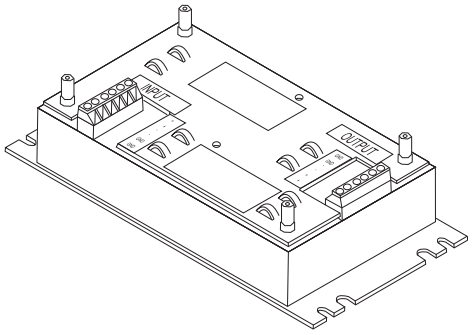
For use with Honeywell power supplies

- 9000301PWRSPLY – Power Supply, 18-60VDC with cable
- 9000302PWRSPLY – Power Supply, 60-110VDC with cable:



Shown With Lid Attached

- Lid is secured with screws on the top of lid.



Shown With Lid Removed

- Input and output connector blocks under lid.
- Two positive (+), negative (-) and ground (⏚) connections per terminal block

If your DC to DC power supply does not look like the image above, see DC/DC Power Supply Installation, Screws on Side of Lid (page 14-29) for installation instruction.

Connecting Electrical Cables to Power Sources

The DC to DC power supply is used to provide vehicle power to the MX7 Tecton when placed in a DC powered vehicle cradle.

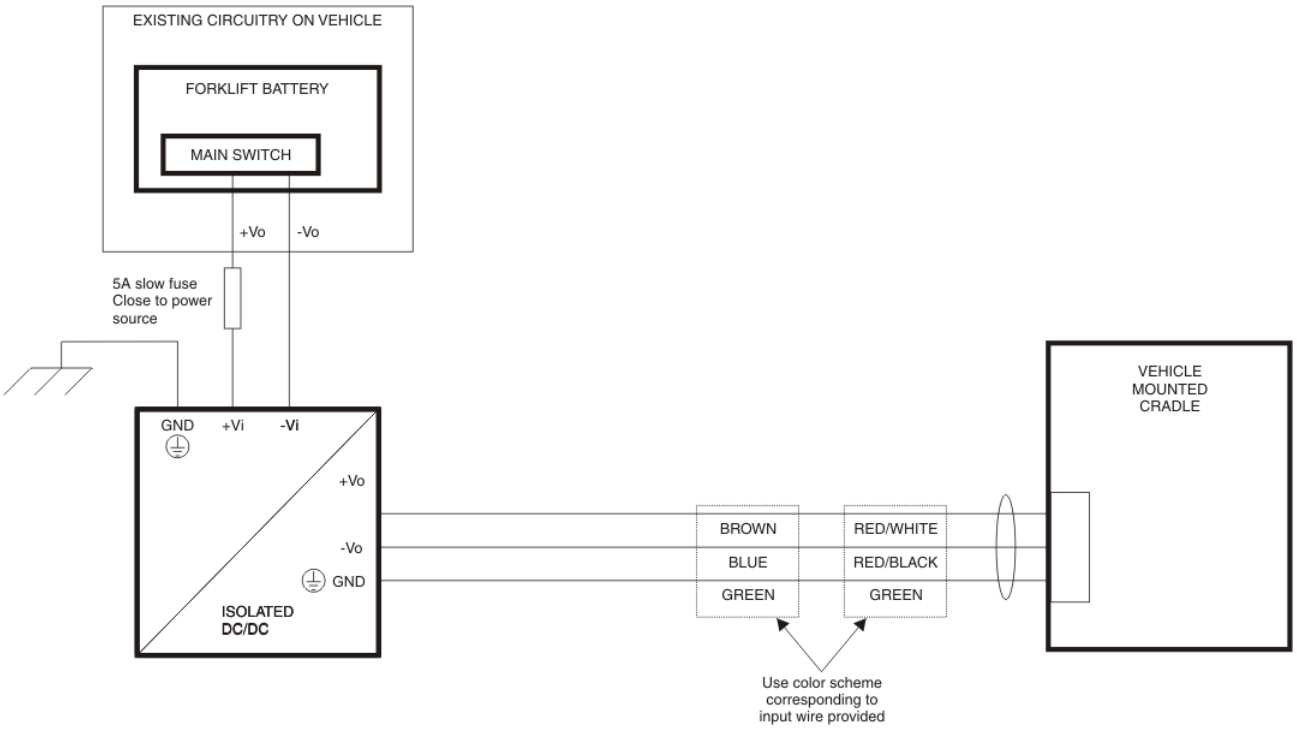
Specifications for Electrical Supply

Input Voltage	Always observe input voltage range specified on the DC to DC power supply.
Output Voltage	12 VDC ± 10%
Power	60 W
Fuse	5 A (slow blow fuse). Fuses are USER SUPPLIED

Note: Refer to the Wiring Schematic that follows for wiring colors and connections.

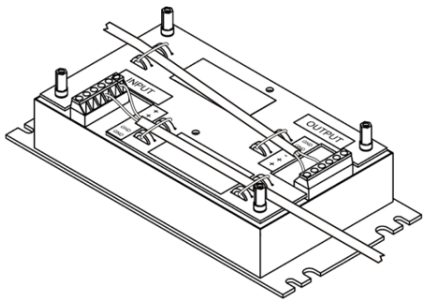
Caution: ⚠	For proper and safe installation, the input power cable must be connected to a fused circuit on the vehicle. This fused circuit requires a five Amp maximum time delay (slow blow) high interrupting rating fuse. If the supply connection is made directly to the battery, the fuse should be installed in the positive lead within 5 inches of the battery positive (+) terminal. Note: For North America, a UL Listed fuse is to be used.
Caution: ⚠	Usage in areas where moisture can affect the power supply connections should be avoided. The power supply should be mounted in a dry location within the vehicle or placed in a suitable protective enclosure.
Caution: ⚠	For installation by trained service personnel only.
Warning: ⚠	Risk of ignition or explosion. Explosive gas mixture may be vented from battery. Work only in well ventilated area. Avoid creating arcs and sparks at battery terminals.

Wiring Schematic



Connecting Vehicle Electrical Supply

1. The vehicle cradle must be empty.
2. Begin by connecting the power cable to the vehicle cradle. Work from this connection with the last connection being to the vehicle's power source.
3. Route the cable from the cradle to the DC to DC power supply.
4. Cut the cable to length and strip the wire ends. Route the power cable the shortest way possible. The cable is rated for a maximum temperature of 105°C (221°F). When routing this cable it should be protected from physical damage and from surfaces that might exceed this temperature. Do not expose the cable to chemicals or oil that may cause the wiring insulation to deteriorate. Always route the cable so that it does not interfere with safe operation and maintenance of the vehicle.
5. Remove the lid from the DC to DC power supply by removing only the screws on the top of the lid.
6. Attach the stripped wire ends to the output side of the DC to DC power supply.
7. Attach the stripped wire ends to the input side of the DC to DC power supply.
8. The input and output blocks each have two + plus and two – minus connectors. Either connector in the block can be used to connect the matching polarity wire. The input and output blocks also each have two chassis ground connections. When connecting the cradle to vehicle power, use one chassis ground connector in each block.



9. Wire colors depend on the type of device attached. Please refer to the Wiring Schematic for wire colors.
10. Use the looms and wire ties to secure all wiring as shown above, then reattach the lid.
11. Connect the DC to DC power supply to the vehicle's electrical system as directed below:.

Caution: 	**For battery powered vehicles:** VIN+ is connected to battery positive. VIN- must be connected to battery negative. ⏚ must be connected to the vehicle chassis ground. **For internal combustion engine powered vehicles:** VIN+ is connected to battery positive. VIN- is connected to battery negative. ⏚ is connected to the vehicle chassis ground, which can also be battery negative.

12. While observing the fuse requirements shown in Specifications for Electrical Supply, connect the power cable as close as possible to the actual battery terminals of the vehicle. When available, always connect to unswitched terminals in the vehicle fuse panel, after providing proper fusing.

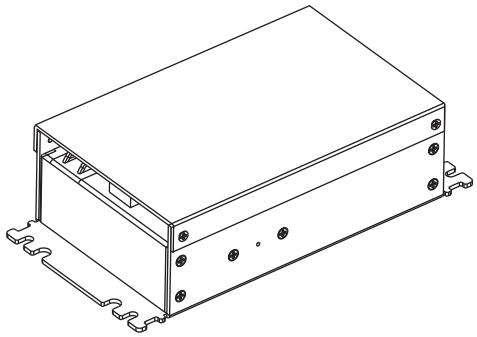
    ATTENTION: For uninterrupted power, electrical supply connections should not be made at any point after the ignition switch of the vehicle.

13. Use proper electrical and mechanical fastening means for terminating the cable. Properly sized "crimp" type electrical terminals are an accepted method of termination. Select electrical connectors sized for use with 18AWG (1mm2) conductors.
14. Provide mechanical support for the cable by securing it to the vehicle structure at approximately one foot intervals, taking care not to over tighten and pinch conductors or penetrate the outer cable jacket.

DC/DC Power Supply Installation, Screws on Side of Lid

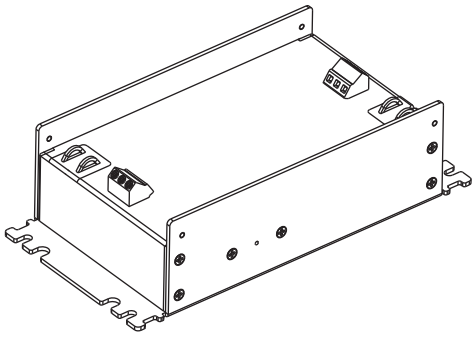
For use with

- 9000311PWRSPLY – Power Supply, 9-60VDC, 60W
- 9000313PWRSPLY – Power Supply, 50-150VDC, 60W:



Shown With Lid Attached

- Lid is secured with screws on the side of lid.



Shown With Lid Removed

- Input and output connector blocks under lid.
- One positive (Vin+), negative (Vin-) and ground (⏚) connection in input block.
- One positive (Vo+) and negative (Vo-) connection in output block.

If your DC/DC power supply does not look like the image above, see DC/DC Power Supply Installation, Screws on Top of lid (page 14-26) for installation instruction.

Connecting Electrical Cables to Power Sources

The DC/DC power supply is used to provide vehicle power to the MX9 when it is placed in a DC powered vehicle cradle.

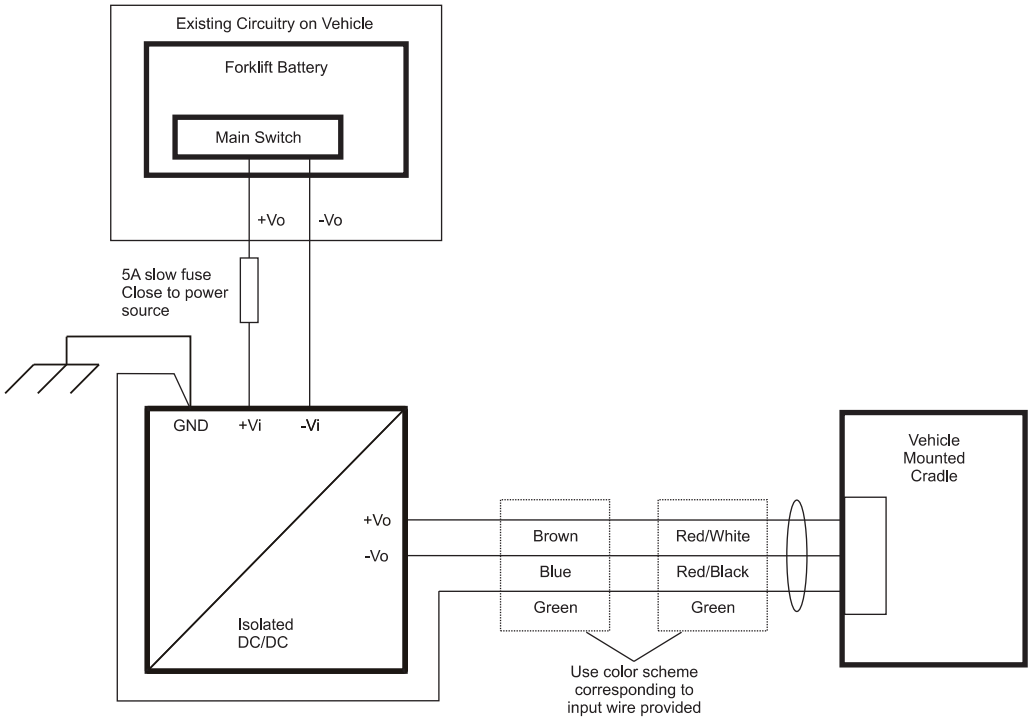
Specifications for Electrical Supply

Input Voltage	Always observe input voltage range specified for the DC/DC power supply.
Output Voltage	13.5 VDC ± 10%
Fuse	5 A (slow blow fuse). Fuses are USER SUPPLIED

Note: Refer to the Wiring Schematic that follows for wiring colors and connections.

Caution: ⚠	For proper and safe installation, the input power cable must be connected to a fused circuit on the vehicle. This fused circuit requires a five Amp maximum time delay (slow blow) high interrupting rating fuse. If the supply connection is made directly to the battery, the fuse should be installed in the positive lead within 5 inches of the battery positive (+) terminal. Note: For North America, a UL Listed fuse is to be used.
Caution: ⚠	Usage in areas where moisture can affect the power supply connections should be avoided. The power supply should be mounted in a dry location within the vehicle or placed in a suitable protective enclosure.
Caution: ⚠	For installation by trained service personnel only.
Warning: ⚠	Risk of ignition or explosion. Explosive gas mixture may be vented from battery. Work only in well ventilated area. Avoid creating arcs and sparks at battery terminals.

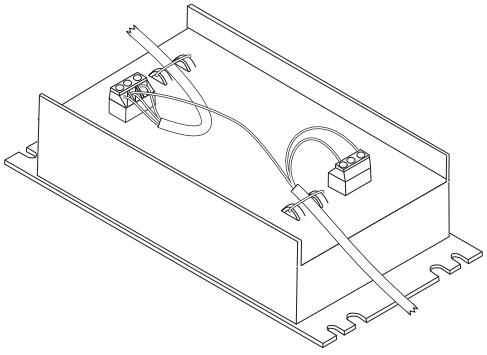
Wiring Schematic



Connecting to Vehicle Power

The vehicle cradle must be empty. The last connection must be to the vehicle power source.

1. Connect the power cable to the vehicle cradle.
2. Route the cable from the cradle to the DC/DC power supply.
3. Cut the cable to length and strip the wire ends.
4. Route the power cable the shortest way possible. The cable is rated for a maximum temperature of 105°C (221°F). When routing this cable it should be protected from physical damage and from surfaces that might exceed this temperature. Do not expose the cable to chemicals or oil that may cause the wiring insulation to deteriorate. Always route the cable so that it does not interfere with safe operation and maintenance of the vehicle.
5. Remove the lid from the DC/DC power supply by removing only the screws on the side of the lid.
6. Attach the stripped wire ends to the output side of the DC/DC power supply



.

Note: The input block has V_{IN+}, V_{IN-} and GND terminals. The output block has V_{O+} and V_{O-} terminals.

7. Connect the ground wire from the cradle to the GND terminal on the input side of the DC/DC power supply.

8. Route the wiring from the DC/DC power supply to the vehicle's electrical system. **Do not connect to vehicle power at this time.**
9. Strip the wire ends and connect to the input side of the DC/DC power supply.
10. Use looms and wire ties to secure all wiring as shown.
11. Reattach the cover with the screws.
12. Connect the DC/DC power supply to the vehicle's electrical system as directed below:

Caution: 	**For battery powered vehicles:** VIN+ is connected to battery positive. VIN- must be connected to battery negative.  must be connected to the vehicle chassis ground. **For internal combustion engine powered vehicles:** VIN+ is connected to battery positive. VIN- is connected to battery negative.  is connected to the vehicle chassis ground, which can also be battery negative.

13. While observing the fuse requirements specified above, connect the power cable as close as possible to the actual battery terminals of the vehicle. When available, always connect to unswitched terminals in the vehicle fuse panel, after providing proper fusing.

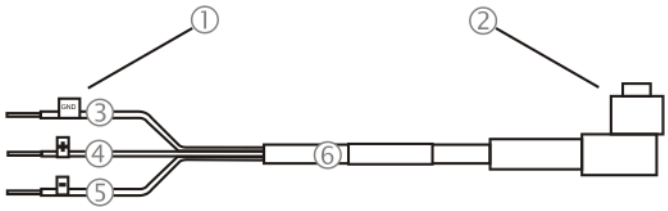
    ATTENTION: For uninterrupted power, electrical supply connections should not be made at any point after the ignition switch of the vehicle.
14. Use proper electrical and mechanical fastening means for terminating the cable. Properly sized "crimp" type electrical terminals are an accepted method of termination. Select electrical connectors sized for use with 18AWG ($1mm^2$) conductors.
15. Provide mechanical support for the cable by securing it to the vehicle structure at approximately one foot intervals, taking care not to over tighten and pinch conductors or penetrate the outer cable jacket.

Vehicle 12V Bare Wire Adapter

Part Number: 9000A079CBL12ML3

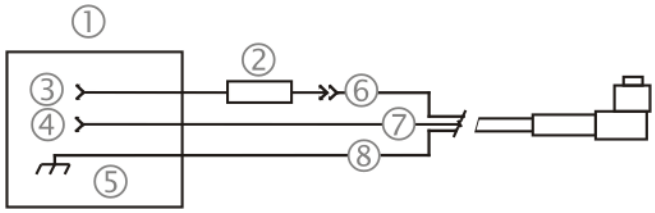
Caution: 	For proper and safe installation, the input power cable must be connected to a fused circuit on the vehicle. This fused circuit requires a ten Amp maximum time delay (slow blow) high interrupting rating fuse. If the supply connection is made directly to the battery, the fuse should be installed in the positive lead within 5 inches of the battery positive (+) terminal. Note: For North America, a UL Listed fuse is to be used.
Caution: 	For installation by trained service personnel only.

Vehicle Cable Connection Cable (Fuse Not Shown)



1. To Vehicle Battery
2. To Vehicle Mounted Device
3. Green (GND)
4. Brown (DC+)
5. Blue (DC-)
6. 12 VDC

Connecting the Power Cable to the Vehicle



1. Vehicle Electrical System
2. 10 Amp Slow Blow Fuse
3. DC +
4. DC -
5. Vehicle Chassis
6. Brown
7. Blue
8. Green

Note: Correct electrical polarity is required for safe and proper installation. The cradle will not power on or function if the cable is connected with the polarity reversed. See the following figure titled "Vehicle Connection Wiring Color Codes" for additional wire color-coding specifics.

Connecting Vehicle 12 VDC Supply

1. The power cable must be UNPLUGGED from the MX7 Tecton vehicle cradle.
2. While observing the fuse requirements specified above, connect the power cable as close as possible to the actual battery terminals of the vehicle. When available, always connect to unswitched terminals in the vehicle fuse panel, after providing proper fusing.
3. ATTENTION: For uninterrupted power, electrical supply connections should not be made at any point after the ignition switch of the vehicle.
4. Route the power cable the shortest way possible. The cable is rated for a maximum temperature of 105°C (221°F). When routing this cable it should be protected from physical damage and from surfaces that might exceed this temperature. Do not expose the cable to chemicals or oil that may cause the wiring insulation to deteriorate.
5. Always route the cable so that it does not interfere with safe operation and maintenance of the vehicle.

6. Use proper electrical and mechanical fastening means for terminating the cable. Properly sized “crimp” type electrical terminals are an accepted method of termination. Select electrical connectors sized for use with 18AWG (1mm2) conductors.
7. Wiring color codes for Honeywell supplied DC input power cabling:

Vehicle Supply		Wire Color
+12 VDC	DC +	Brown
Return	DC -	Blue
Vehicle Chassis	GND	Green

8. Provide mechanical support for the cable by securing it to the vehicle structure at approximately one foot intervals, taking care not to over tighten and pinch conductors or penetrate outer cable jacket.
9. Refer to the following sections to complete the power connection to the MX7 Tecton vehicle cradle.

Connecting Power Supply to Vehicle Cradle

Note: When an external power supply is used to power this cradle, the external power supply should be UL Listed, with LPS or Class 2 outputs rated 12V, minimum 2 Amps.

The power cable connector is L-shaped. The long end of the L (the cable) will be facing up towards the middle strain relief cable clamp. The Power port is on the back of the cradle.

1. Align the connector pins to the vehicle cradle Power connector; firmly pushing the connector into the Power port.
2. Tighten the nut of the plug clockwise until the power cable is securely fastened.
3. Secure the cable to the cradle with the strain relief cable clamps, see Vehicle Cradle Strain Relief Cable Clamps (page 14-34).
4. The power LED on the MX7 Tecton illuminates when it is receiving external power and the MX7 Tecton is docked.

Attaching a Serial or I/O Connector

The serial cable is connected to the port labeled Serial Interface on the back of the vehicle cradle.

The serial cable can originate with a tethered scanner, a PC, a printer or another serial device.

The I/O connector cable is connected to the port (male) labeled MX7 Tecton I/O Port on the back of the vehicle cradle.

Periodically test the connections for stability and re-tighten if necessary.

Serial Port

1. Align the RS232 serial cable end (female) carefully to the Serial Interface port (male) at the back of the cradle.
2. Firmly press the ends together and finger tighten the screws on either side of the connector. Test the connection for stability.
3. Secure the cable to the cradle with one of the strain relief cable clamps on the back of the vehicle cradle.

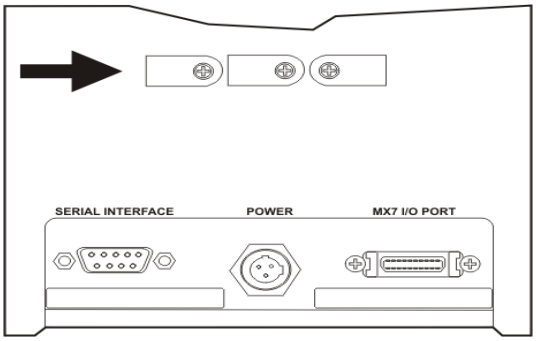
I/O Port

1. Squeeze the clips next to the connector attached to the I/O cable to open the catches in the connector assembly.
2. Firmly press the cable end (female) into the I/O Port connector (male) at the back of the cradle. Release the clips in the connector cable. Test the connection for stability.
3. Secure the cable to the cradle with one of the strain relief cable clamps on the back of the vehicle cradle.

Vehicle Cradle Strain Relief Cable Clamps

Equipment Required: Phillips screwdriver (not supplied by Honeywell).

There are three strain relief cable clamps secured to the back of the vehicle cradle, located above the ports for the Serial Interface, Power and MX7 I/O connections.



1. Remove the strain relief cable clamp from the back of the cradle by turning the screw counterclockwise. Put the screw aside in a safe location.
2. Slide the strain relief clamp over the cable.
3. Using a Phillips screwdriver and the screw that was removed, refasten the clamp holding the cable to the vehicle cradle. Do not stretch the cable. Leave enough slack in the cable to allow the cable to be connected and disconnected from the MX7 Tecton easily when needed.
4. Continue in this manner until all cables are secured to the back of the vehicle cradle.

Vehicle Cradle LED

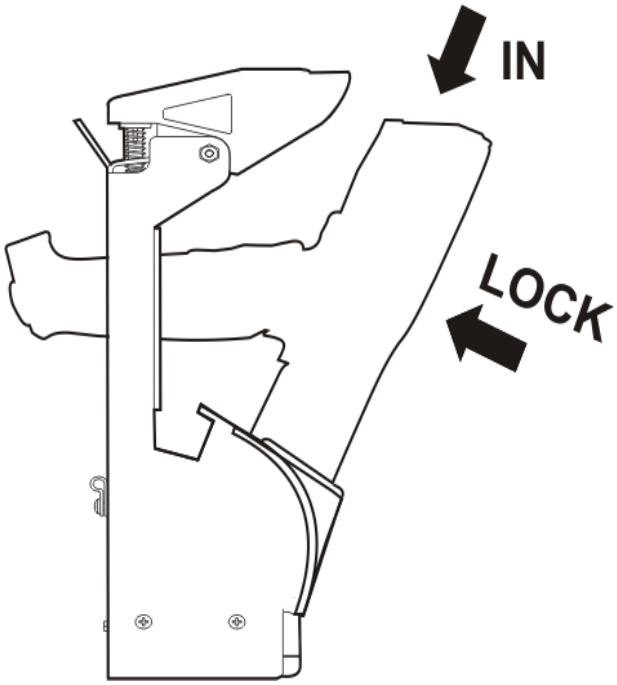
The cradle LED is located at the front center of the cradle.

When Cradle LED is …	It means ….
 Off	MX7 Tecton is docked. Cradle does not have power. MX7 Tecton is not docked. Cradle may have power. Check the power connector at the back of the cradle.
 Red	MX7 Tecton is docked and external power is connected.

Docking the MX7 Tecton in a Powered Vehicle Cradle

Note: Do not put the MX7 Tecton into the vehicle cradle until the cradle is securely fastened to the vehicle. Always put the handle through the Handle Opening first or damage to the scanner aperture may occur.

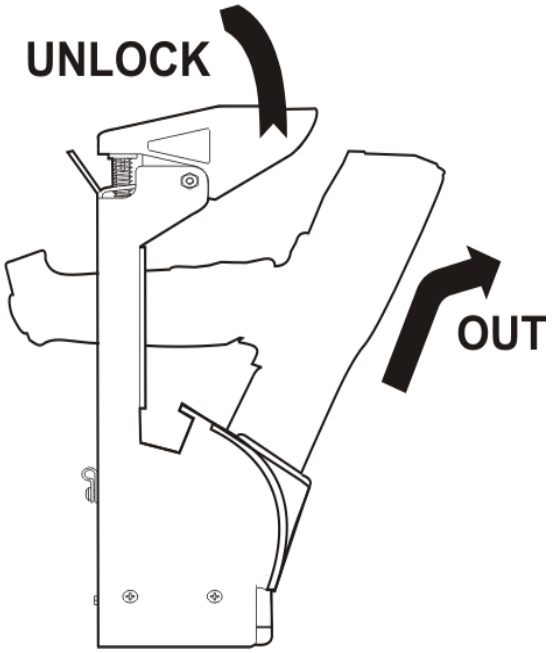
1. The MX7 Tecton is inserted into the cradle by pressing the base of the MX7 Tecton down into the cradle pocket until the connector at the base of the MX7 Tecton clicks into place with the charging connector at the bottom of the docking well.
2. If the cradle is connected to a power source, the Docked LED illuminates.
3. Firmly press the MX7 Tecton backward until the Retainer snaps forward, its latches catching on the front of the MX7 Tecton, securing it in the cradle.



Do not slam the MX7 Tecton into the cradle pocket. Damage to the cradle and MX7 Tecton components may occur. If the vehicle cradle or MX7 Tecton is damaged, it must be removed from service and repaired before placing it into service again.

Removing the MX7 Tecton from a Powered Vehicle Cradle

1. Push the top of the Retainer up and back until the MX7 Tecton is released from the Retainer latches and the charging pocket swings forward.



2. Pull the MX7 Tecton up and out of the vehicle cradle pocket, disconnecting the MX7 Tecton from the charge/ communication port at the base of the docking bay. The Docked LED turns off.

Powered Vehicle Cradle Help

The following is intended as an aid in determining whether the MX7 Tecton or the vehicle mounted cradle may be malfunctioning.

Problem	Cause	Solution
MX7 Tecton docked in cradle but cannot work with accessory cables connected to cradle.	MX7 Tecton not fully seated in cradle. There are foreign objects inside docking bay or cable connectors	Reseat the MX7 Tecton fully into the docking bay. Remove the foreign objects and reseat the MX7 Tecton in the docking bay.
MX7 Tecton docked in cradle but Docked LED does not light up.	MX7 Tecton not fully docked. Power supply not connected.	Check the docking bay is clear of foreign objects and reseat the MX7 Tecton fully into the docking bay. Check that power is connected to the Power Port at the rear of the cradle.

15 Technical Specifications

MX7 Tecton Hardware

Processor	Marvell PXA-320 CPU operating at 806 MHz. Turbo mode switching is supported. 32 bit CPU (with on-chip cache)
Memory	DRAM: 256 MB DDRAM | 256MB NAND Flash
Mass Storage	One SD Memory card slot for Expansion Memory : Options: 1GB, 4GB
Operating System	Microsoft® Windows® Mobile® 6.5
Radio Modules	802.11 a/b/g radio / Bluetooth
Scanner options	Integrated. No Scanner Symbol SE1524ER Lorax Symbol SE955I (Short Range) Symbol SE955E (Base Laser) Hand Held Products 5300 2D Imager Honeywell Laser Scanner, N43XX Honeywell Laser Scanner, N73XX
Display	Transmissive Color LCD. Touch screen. Customer Configurable Display. Backlighting. Indoor readable. Type - LCD – Active Transmissive Color / LED Backlight Resolution - 320 (Vertical) x 240 (Horizontal) pixels Size - 1/4 VGA portrait Diagonal Viewing Area - 3.5 in (8.9cm) Dot Pitch - 0.22mm Dot Size - 0.20mm x 0.20mm Color Scale - Reflective – 256 colors
External Connectors / Interface	RS232 COM1 mini D serial port. 20 Position “D” (female) Connector. Provides cabled connection to external devices such as an audio headset, printer, USB/power connection, RS232/power connection.
Main Battery	Standard: Li-Ion battery pack 7.4V 2200mAh.In-Unit and External Re-Chargeable Cold Storage: Li-Ion battery pack 7.4V 1250mAh.In-Unit and External Re-Chargeable
Backup Power	2.5V Super-capacitor (Super-cap). No backup “battery” is used.

MX7 Tecton Dimensions and Weight

Dimension	
Length	8.8” | 22.3 cm
Width at Display Width at handgrip	3.4” | 8.6 cm 2.8” | 7.1 cm
Depth at Scanner Depth at Battery	2” | 5.1 cm 1.7” | 4.3 cm
Weight	
Unit with network card, battery, SE1524ER scanner and handle	1.6 lbs (26.1 oz) | 740g
Unit with network card, battery, SE1524ER scanner and handstrap	1.4 lbs (22.6 oz) | 640g
Battery	4.3 oz | 122g
Handle	4 oz | 110g
Network Card	0.35 oz | 9.9g
SD Flash Card	1 oz | 28g

MX7 Tecton Environmental Specifications

Operating Temperature	14°F to 122°F (-10°C to 50°C)
Storage Temperature	-4°F to 158°F (-20°C to 70°C)
ESD	8 KV air, 4kV direct contact
Freezer Operating Temperature	-30°C to 60°C
Operating Humidity	Up to 90% non-condensing at 104°F (40°C)
Water and Dust	IEC 60529 compliant to IP65
Vibration	Based on MIL Std 810D

MX7 Tecton Network Card Specifications

Summit 802.11 a/b/g SDIO 2.4/5.0GHz

Wireless Frequencies	2.4 to 2.4897 GHz IEEE 802.11b / 802.11g DSSS OFDM 5.0GHz IEEE 802.11a DSSS OFDM
RF Data Rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
RF Power Level	64 mW (18dBm)
Channels	FCC: 1-11, 36, 40 ,44, 48, 149, 153, 157, 161 ETSI: 1-13, 36, 40, 44 ,48
Operating Temperature	Same as MX7 Tecton Operating Temperature.
Storage Temperature	Same as MX7 Tecton Storage Temperature.
Connectivity	TCP/IP, Ethernet, ODI
Diversity	Yes

Bluetooth

Connection	No more than 32.80 feet (10 meters) line of sight
Operating Frequency	2.402 – 2.480 GHz
Bluetooth Version	2.1 + EDR

MX7 Tecton AC/DC Wall Adapter

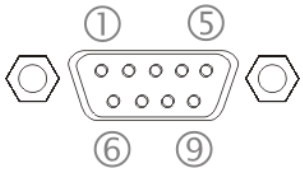
Input Power Switch	None
Power “ON” Indicator	None
Input Fusing	Thermal Fuse
Input Voltage	100VAC min – 240 VAC max
Input Frequency	50 - 60 Hz
Input Connector	North American wall plug, no ground
Output Connector	AC wall adapter has a 5.5mm barrel connector. This connects to the cables which transition power to the 20 pin D connector.
Output Voltage	+12V, regulated
Output Current	0 Amps min, 1.25 Amps max

Operating Temperature	32 F to 100° F / -0° C to 40° C The AC Power Adapter is only intended for use in a 25°C (77°F) maximum ambient temperature environment.
Storage Temperature	-40° F to 180° F / -40° C to 80° C
Humidity	Operates in a relative humidity of 5 – 95% (non-condensing)

Desktop Cradle

Weight	18 oz / 500 grams
Dimensions	H 3.5 in x W 4.25 in x L 7.5 in
Temperature	
Operating	32° F to 104° F / 0° C to 40° C (charger On, no charging in progress)
Charging	50° F to 104° F / 10° C to 40° C (spare battery charger is charging)
Storage	-4° F to 158° F / -20° C to 70° C
Humidity	5% to 90% (non-condensing) at 104° F / 40° C
IEC 60529	Compliant to IP40
Ports	Power, MX7 Tecton Input/Output and serial port

Serial Port



The connector is industry-standard RS232 and is a PC/AT standard 9-pin D male connector.

Note: Tethered scanners must be connected to powered cradles.

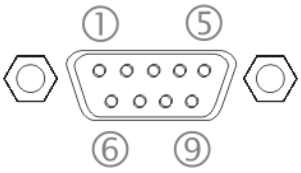
Pin	Signal	Description
1	DCD	Data Carrier Detect
2	RXD	Received Data – Input
3	TXD	Transmitted Data – Output
4	DTR	Data Terminal Ready
5	GND	Signal/Power Ground
6	DSR	Data Set Ready
7	RTS	Request to Send
8	CTS	Clear To Send
9	RI or Power	+5 VDC sourced by the Cradle

Note: Pin 9 of this port is connected to +5 VDC and only approved Honeywell cables are to be used for communication between the cradle and external devices.

Vehicle Mounted Cradle

Weight	2 lbs. 15.2 oz / 1.34 kg
Dimensions	Height 12.5 in. (31.8 cm) Width 6.0 in. (15 cm) Depth 5.0 in. (13 cm)
Operating Temperature	14° F to 122° F (-10° C to 50° C)
Storage Temperature	-4° F to 158° F (-20° C to 70° C)
Humidity	5% to 90% (non-condensing) at 104° F / 40° C

Serial Port



The connector is industry-standard RS232 and is a PC/AT standard 9-pin D male connector.

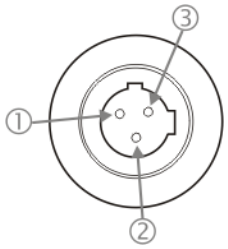
Note: Tethered scanners must be connected to powered cradles.

Pin	Signal	Description
1	DCD	Data Carrier Detect
2	RXD	Received Data – Input
3	TXD	Transmitted Data – Output
4	DTR	Data Terminal Ready
5	GND	Signal/Power Ground
6	DSR	Data Set Ready
7	RTS	Request to Send
8	CTS	Clear To Send
9	RI or Power	+5 VDC sourced by the Cradle

Note: Pin 9 of this port is connected to +5 VDC and only approved Honeywell cables are to be used for communication between the cradle and external devices.

Power Connector Port

Note: When an external power supply is used to power these products, the external power supply should be UL Listed, with LPS or Class 2 outputs rated 12V, minimum 2 Amps.



Pin	Signal	Wire Color
1	Ground (CG)	Green
2	Return (-)	Blue
3	+12V (+)	Brown

The Power connector is located on the back of the vehicle cradle.

Battery Charger

Battery: MX7 Tecton Li-Ion 7.4V 2.2Ah battery with a 500 charge/discharge life cycle.

Electrical

Note: Battery packs may leak up to 1mA current through the battery contacts when left in a non-powered battery charger charging pocket.

Parameter	Minimum	Maximum	Note
Power Supply Input Voltage (V AC-IN)	100 VAC	240VAC	Auto-switching
Power Supply Input Frequency (freq)	47Hz	63Hz	

Temperature

Function	Minimum	Maximum	Note
Operating	0°C (32°F)	+40°C / (104°F)	
Battery Pack Charging	0°C (32°F)	+40°C / (104°F)	Battery packs will not begin charging when their internal temperature is outside this range.
Storage	-20°C (-4°F)	+70°C / (160°F)	Unit is off.

Dimensions

Category	Dimension
Weight	1.75 lbs / .79 kg
Length	12.25” / 31.1 cm
Width	5.25” / 13.3 cm
Height	1.5” / 4 cm
Plug Type	IEC320 (3 prong, grounded)

16 Customer Support

Technical Assistance

If you need assistance installing or troubleshooting your device, please contact us by using one of the methods below:

Knowledge Base: www.hsmknowledgebase.com

Our Knowledge Base provides thousands of immediate solutions. If the Knowledge Base cannot help, our Technical Support Portal (see below) provides an easy way to report your problem or ask your question.

Technical Support Portal: www.hsmsupportportal.com

The Technical Support Portal not only allows you to report your problem, but it also provides immediate solutions to your technical issues by searching our Knowledge Base. With the Portal, you can submit and track your questions online and send and receive attachments.

Web form: www.hsmcontactsupport.com

You can contact our technical support team directly by filling out our online support form. Enter your contact details and the description of the question/problem.

Telephone: www.honeywellaidc.com/locations

For our latest contact information, please check our website at the link above.

Product Service and Repair

Honeywell International Inc. provides service for all of its products through service centers throughout the world. To obtain warranty or non-warranty service, please visit www.honeywellaidc.com and select Support > Contact Service and Repair to see your region's instructions on how to obtain a Return Material Authorization number (RMA #). You should do this prior to returning the product.

Limited Warranty

Honeywell International Inc. ("HII") warrants its products to be free from defects in materials and workmanship and to conform to HII's published specifications applicable to the products purchased at the time of shipment. This warranty does not cover any HII product which is (i) improperly installed or used; (ii) damaged by accident or negligence, including failure to follow the proper maintenance, service, and cleaning schedule; or (iii) damaged as a result of (A) modification or alteration by the purchaser or other party, (B) excessive voltage or current supplied to or drawn from the interface connections, (C) static electricity or electrostatic discharge, (D) operation under conditions beyond the specified operating parameters, or (E) repair or service of the product by anyone other than HII or its authorized representatives.

This warranty shall extend from the time of shipment for the duration published by HII for the product at the time of purchase ("Warranty Period"). Any defective product must be returned (at purchaser's expense) during the Warranty Period to HII factory or authorized service center for inspection. No product will be accepted by HII without a Return Materials Authorization, which may be obtained by contacting HII. In the event that the product is returned to HII or its authorized service center within the Warranty Period and HII determines to its satisfaction that the product is defective due to defects in materials or workmanship, HII, at its sole option, will either repair or replace the product without charge, except for return shipping to HII.

EXCEPT AS MAY BE OTHERWISE PROVIDED BY APPLICABLE LAW, THE FOREGOING WARRANTY IS IN LIEU OF ALL OTHER COVENANTS OR WARRANTIES, EITHER EXPRESSED OR IMPLIED, ORAL OR WRITTEN, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

HII'S RESPONSIBILITY AND PURCHASER'S EXCLUSIVE REMEDY UNDER THIS WARRANTY IS LIMITED TO THE REPAIR OR REPLACEMENT OF THE DEFECTIVE PRODUCT WITH NEW OR REFURBISHED PARTS. IN NO EVENT SHALL HII BE LIABLE FOR INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, AND, IN NO EVENT, SHALL ANY LIABILITY OF HII ARISING IN CONNECTION WITH ANY PRODUCT SOLD HEREUNDER (WHETHER SUCH LIABILITY ARISES FROM A CLAIM BASED ON CONTRACT, WARRANTY, TORT, OR OTHERWISE) EXCEED THE ACTUAL AMOUNT PAID TO HII FOR THE PRODUCT. THESE LIMITATIONS ON LIABILITY SHALL REMAIN IN FULL FORCE AND EFFECT EVEN WHEN HII MAY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH INJURIES, LOSSES, OR DAMAGES. SOME STATES, PROVINCES, OR COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATIONS OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

All provisions of this Limited Warranty are separate and severable, which means that if any provision is held invalid and unenforceable, such determination shall not affect the validity of enforceability of the other provisions hereof. Use of any peripherals not provided by the manufacturer may result in damage not covered by this warranty. This includes but is not limited to: cables, power supplies, cradles, and docking stations. HII extends these warranties only to the first end-users of the products. These warranties are non-transferable.

The duration of the limited warranty for the MX7 Tecton is 1 year.

The duration of the limited warranty for the MX7 Tecton Desktop Cradle is 1 year.

The duration of the limited warranty for the MX7 Tecton Vehicle Cradle is 1 year.

The duration of the limited warranty for the MX7 Tecton Passive Vehicle Cradle is 1 year.

The duration of the limited warranty for the MX7 Tecton Battery Charger is 1 year.

The duration of the limited warranty for the MX7 Tecton 2200mAh Li-Ion and 1250mAh Li-Ion Battery is 6 months.

The duration of the limited warranty for the MX7 Tecton AC power supply and cables is 1 year.

The duration of the limited warranty for the MX7 Tecton DC-DC Converter and cable is 1 year.

The duration of the limited warranty for the MX7 Tecton cables (USB, Serial, Communication, Power) is 1 year.

The duration of the limited warranty for the MX7 Tecton fabric accessories (e.g., belt, case, holster) is 90 days.

The duration of the limited warranty for the MX7 Tecton headset is 1 year.

Honeywell Scanning & Mobility
9680 Old Bailes Road
Fort Mill, SC 29707

www.honeywellaidc.com